CSB

Report to the Senate Special Committee on the Year 2000 Technology Problem

March 1999

Year 2000 Issues

Technology Problems and Industrial Chemical Safety

U. S. Chemical Safety and Hazard Investigation Board

2175 K Street N.W., 4th Floor, Washington, D.C. 20037
Phone 202-261-7600 Fax 202-261-7650

Dr. Paul L. Hill, Jr.
Chairman and CEO

March 15, 1999

The Honorable Robert Bennett, Chairman
The Honorable Christopher Dodd, Vice Chairman
Special Committee on the Year 2000 Technology Problem
United States Senate
Washington, D.C. 20510-6486

Dear Senators Bennett and Dodd:

The United States Chemical Safety and Hazard Investigation Board (CSB), at the request of the U.S. Senate Special Committee on the Year 2000 Technology Problem, is hereby transmitting to the Special Committee its report entitled "The Year 2000 Technology Problem and Chemical Safety".

On November 2, 1998, you requested the CSB to convene a meeting with chemical producers, users, and other impacted parties, examine the safety impact of the Y2K technology problem on chemical safety within the United States, and report back to the Special Committee regarding its findings.

Under the direction of Dr. Gerald Poje, a Board Member, a meeting of over 40 interested parties was convened on December 18, 1998. The attached report, also prepared under the direction of Dr. Poje, represents input from those attendees. The report's findings, conclusions and recommendations have been reviewed and accepted by the full Board.

Should you have questions regarding the content of the report, please contact me by telephone at (202) 261-7600.

Sincerely,

Paul L. Hill, Jr., Ph.D.
Chairman and Chief Executive Officer

BY THE CHEMICAL SAFETY AND HAZARD INVESTIGATION BOARD

Paul L. Hill, Jr.
Chairman

Gerald V. Poje
Member

Andrea Kidd Taylor
Member

Isadore Rosenthal
Member

March 11, 1999

Acknowledgement

The U.S. Senate Special Committee on the Year 2000 Technology Problem requested the U.S. Chemical Safety and Hazard Investigation Board prepare this report. The Board Members recognize the leadership and diligence of The Mary Kay O'Connor Process Safety Center at Texas A&M University in this process. Professor Sam Mannan provided expert assistance in the overall research and development of this report. Mr. Charles Isdale coordinated the evaluation of process controls and other equipment, and Mr. Jerry Bradshaw coordinated evaluation of plant operations issues.

Contents

Contents

Abbreviations

AIChE	American Institute of Chemical Engineers
API	American Petroleum Institute
ASSE	American Society of Safety Engineers
CAA	Clean Air Act
CMA	Chemical Manufacturers Association
CSB	Chemical Safety Board
EPA	Environmental Protection Agency
HAZMAT	Hazardous Materials
ISA	International Society for Measurement and Control
NIEHS	National Institute of Environmental Health Services
OECD	Organization of Economic Cooperation and Development
OSHA	Occupational Safety and Health Administration
SEC	Securities and Exchange Commission
SME	Small and Mid-Sized Enterprises
Y2K	Year 2000

Background and Results

On December 18, 1998, at the request of the U.S. Senate Special Committee on the Year 2000 Technology Problem, Dr. Gerald Poje, one of Chemical Safety and Hazard Investigation Board's Board Members convened a Year 2000 (Y2K) workshop (Appendix I). The workshop brought together professionals from the public and private sectors for the purpose of drawing on the participants' expertise in order to assess the impact of the Y2K problem with regard to catastrophic events in the chemical process plants. Appendix II contains a copy of the workshop agenda and a list of those individuals who attended.

Issues addressed by the workshop were limited to safe and continuous production, storage, and distribution of chemicals critical to a range of American industries. The invited participants examined the impact of Y2K failures vis-à-vis process control and automation within the process industry, looking specifically at those areas the Committee requested be evaluated:

- The extent of the Y2K problem as it pertains to the automation systems and embedded systems that monitor or control the manufacture of toxic and hazardous chemicals, or safety systems that protect processes
- The awareness of large, medium, and small companies within the industry of the Y2K threat,
- Their progress to date in addressing the Y2K problem,
- The impact on the Risk Management Plans required in June 1999, and
- The role federal agencies are playing in preventing disasters due to the Y2K problem.

In summary, the Y2K problem is a significant problem in the chemical manufacturing and handling sector. According to the U.S. Environmental Protection Agency (EPA), 85 million Americans live, work and play within a 5-mile radius of 66,000

facilities handling regulated amounts of high hazard chemicals. The following findings were developed as a result of the Technical Workshop:

- Large enterprises with sufficient awareness, leadership, planning, financial and human resources are unlikely to experience catastrophic failures and business continuity problems unless their current progress is interrupted or there are massive failures of utilities.

- The overall situation with small and mid-sized enterprises is indeterminate, but efforts on the Y2K problem appears to be less than appropriate based upon inputs from many experts.

- While the impact of the Risk Management Plans should be positive, there are no special emphases or even specific mention of Y2K technology hazards in either EPA or Occupational Safety and Health Administration (OSHA) regulations regarding process safety.

- Federal agencies are aware of and involved in Y2K technology and chemical safety issues. However, significant gaps exist, and there do not appear to be specific plans to address these gaps.

The Technical Workshop as well as the research conducted for this report concluded that the Y2K problem is one of major proportions and has the potential for causing disruption of normal operations and maintenance at the nation's chemical and petroleum facilities. It is important to point out that Y2K compliance[1] activities reported to the Chemical Safety Board to date have not found a single failure (embedded microchips or software) which by itself could cause a catastrophic chemical accident. However, it is unclear what the outcome might be from multiple failures, e.g., multiple control system failures, multiple utility failures, or a combination of multiple utility and control system failures. Surveillance of the industrial sector that handles high hazard chemicals is insufficient to draw detailed conclusions.

One theme all experts agree on is that failures from Y2K non-compliance at small and mid-sized enterprises is more likely. The reason is a general lack of awareness regarding process safety, and for the Y2K problem in particular, lack of resources and technical know-how for fixing the problems. Given the time constraints, altering this situation would require a massive effort. This effort should focus on: 1. providing easy-to-use tools, 2. promoting accessible resources, and 3. providing attractive incentives for Y2K compliance efforts. Additional efforts should be the focus of an urgent meeting of agencies convened by the administration.

The potential for catastrophic events, at U.S. chemical process plants, stemming from Y2K non-compliance, can be divided into three categories: failures in software or embedded microchips within the process plants, external Y2K-related problems (e.g., power outages), and multiple Y2K-related incidents that may strain emergency response organizations.

The limited scope of the Y2K Technical Workshop and the research conducted for this study concluded that large multinational companies are, in general, following a well-thought out and well-managed path towards Y2K compliance. These multinational enterprises have, in addition to their Y2K compliance efforts, made contingency plans, including, in some cases, plans to shutdown batch operations for limited periods at the turn of the century. These conclusions vis-à-vis large and multinational companies should not be construed to mean that there is no potential for Y2K-related catastrophic events at these facilities. It is possible that some Y2K-impacted components may not have been identified, compliance programs may not achieve 100% completion in time, or multiple failures that may not have been considered may result in accidents.

The major control and instrumentation vendors canvassed in this study are involved in an extensive program to provide Y2K compliance for their products. There is, however, reason to believe that some independent control systems integrators may have developed and implemented control systems for which there is little or no documentation of Y2K-related vulnerabilities. In addition, some vendors are no longer in business or are not as cooperative as the major control and instrumentation vendors.

EPA's Risk Management Program and OSHA's Process Safety Management program mandated by the Clean Air Act Amendments of 1990 may provide significant benefit in terms of improving overall safety programs, reliability of chemical process plants, emergency response plans, and other programs. As a result, the overall capability and readiness of the chemical process industry to deal with and effectively overcome the Y2K threat is very high. However, it must be pointed out that none of these regulatory programs or activities have any direct relationship with Y2K compliance.

Instituting new regulations to standardize testing or certification is not a reasonable approach for three reasons. First, in the remaining time, it is not possible to develop the mechanism and logistics needed for rulemaking, standard development, and establishment of reporting procedures. Second, implementation of any standardized method or regulation may cause penalties and unnecessary complications for many companies that do not fit the selected standard but have already expended an extensive amount of effort on Y2K compliance. Third, it is critical to minimize overall administrative efforts in order to focus available resources on the remedial efforts within this limited time frame.

Special Technical Workshop attendees reached consensus on the importance of four issue areas related to Y2K problems and chemical safety: 1. Small and medium-size enterprises (SMEs) risks and needs, 2. Risk management programs and their applicability, 3. Utility continuity, and 4. Responsive communication among the stakeholders. The following recommendations were developed based on input from the workshop attendees and research conducted during this study.

The administration should promote the development of an information clearinghouse covering chemical process control systems, contingency planning, and other safety-related related Y2K issues. The information should be tailored to specific industry sectors, i.e., propane distributors and users, chlorine facilities (water and wastewater units); and ammonia facilities. Information such as checklists and lists of devices or equipment susceptible to Y2K failures should be provided specific to

industry sectors. A federal government agency should be a focal point for developing and maintaining the clearinghouse in coordination with other public and private entities. For this effort to be successful, the federal government must shield all organizations that are providing Y2K-related information, from the threat of lawsuits.

The President's Council on the Year 2000 should coordinate the development of a contingency planning phase to build public awareness and promote the ability of emergency response infrastructure at the federal, state, and local levels to respond to environmental disruptions, chemical releases, and threats to worker and public health and safety. In this respect, it is critical to coordinate activities with the Federal Emergency Management Agency.

Batch processors should consider delaying batches involving hazardous materials that will be in the process as the clocks turn to 2000, and at other sensitive dates, for processes where testing was not done or testing results were inconclusive.

All processors that will run through the transition should have plans and sufficient and trained staff on hand to manually take control of the process. Facility managers should be prepared to shut down the process quickly and safely should control problems occur. Manual operations, especially over extended periods of time, may require significant changes in staffing and comprehensive training of managers, operators and other workers. The additional training, as appropriate, should be completed early in 1999.

The EPA should promote the development of contingency plans to assure capable emergency response and promote communications among facilities, local governmental agencies and the nearby communities should problems arise.

Facility managers should phase-in and coordinate shut downs, resulting either intentionally as a safeguard against Y2K-related failures or as a direct result of Y2K failures, and startups with local utilities and agencies, including emergency response agencies and Local Emergency Planning Committees.

Chemical workers, emergency responders and local governmental agencies that focus on environmental health and emergency response should be provided with training and tools (e.g., guidelines, checklists, and software) to address Y2K issues.

Power outages and other utility failures could constitute as much of a threat, or even more so, than internal process plant Y2K-related failures. Thus, utilities and oversight agencies should expend every effort to preserve the integrity of the national power grid system, local power supplies and other appropriate utilities. In addition, contingency plans should incorporate specific elements for communicating with utilities regarding each other's status.

Congress should create incentives for Y2K compliance using attractive tax write-offs for Y2K-related spending. This is probably the most effective method for enticing the small and medium-sized enterprises to actively pursue Y2K compliance programs. However, such programs should be developed with appropriate checks and balances to prevent unintended behaviors.

Policy makers should develop small business loans for Y2K compliance with special emphasis on those businesses that are critical to public health and safety. The loans could be provided as low interest loans and could be based on the production or handling of hazardous substances that generate the greatest potential for an impact to workers and the public.

Federal initiatives coordinated through the President's Council on the Year 2000 should include the organization of regional conferences focusing on ways to assess chemical risks appropriately and how to prioritize which systems and facilities pose greater risks.

EPA, OSHA and other safety organizations should increase Y2K awareness in small and mid-sized enterprises (SMEs) by developing outreach campaigns, such as distributing Y2K awareness brochure to everyone on the Toxic Substances Control Act list, and other federal, state and local venues. Instrumentation and control vendors can and should be encouraged to increase

their efforts in this communication activity.

Communication tools should be developed to aid worker and public understanding. While it is critical to develop and implement Y2K compliance programs, it is equally important to inform workers and the public about the extensive work being done, in order to allay fears, avoid panic and promote community contingency planning. In addition, efforts must be continued to communicate the seriousness of Y2K to SMEs and other organizations. This communication can be made through federal agencies, such as EPA, OSHA, and the Chemical Safety and Hazard Investigation Board (CSB), state and local agencies. Other important venues for outreach include: unions, trade and professional organizations, such as the American Institute of Chemical Engineers (AIChE), American Petroleum Institute (API), American Society of Safety Engineers (ASSE), Chemical Manufacturers Association (CMA), Chlorine Institute, and International Society for Measurement and Control (ISA), and research organizations such as the Mary Kay O'Connor Process Safety Center at Texas A&M University.

Multinational Enterprises

The limited scope of this workshop concluded that multinational companies are, in general, following a well-thought out and well-managed path towards Y2K compliance. This involves a close variation of the four-step methodology described later, i.e., identification, assessment, remediation, and testing and certification. These companies have filed their Y2K disclosures, as required by the Securities and Exchange Commission (SEC), which spell out their activities regarding Y2K compliance. The SEC disclosures examined during this study indicate that these multinational enterprises will most likely be in compliance by the new millennium. However, many disclosures express concerns about business continuity in light of uncertainties with externalities.

Others have recommended that the SEC conduct independent audits of the Year 2000 Management Discussion & Analyses to assure those disclosures reflect actual efforts in companies.[2] For the benefit of chemical safety, such disclosures should be available on a facility specific basis and not aggregated across a corporation.

These multinational enterprises have, in addition to their Y2K compliance efforts, made contingency plans, including, in some cases, plans to shutdown batch operations for limited periods at the turn of the century.

These conclusions about large and multinational companies should not be construed to mean that there is no potential for Y2K-related catastrophic events at these facilities. It is possible that some Y2K-impacted components may not have been identified or compliance programs may not be 100% complete in time.

In addition, one of the problems identified from information gathered from the SEC disclosure forms is not necessarily the amount of money committed but the distribution of those resources over time. Some companies have projected the majority of their efforts into 1999, leaving little opportunity to accommodate unanticipated delays.

Small and Mid-sized Enterprises (SMEs)

One of the major concerns regarding Y2K-related catastrophic events may be associated with SMEs. (For the purposes of this report, SMEs are defined as facilities that have less than 50 employees, facilities that have between 51-200 employees or are not part of a multinational national corporation, or public sector facilities, e.g., municipal water and wastewater facilities.) SMEs managing high hazard chemicals can pose large risks to works and the surrounding community. While some exceptional SMEs are highly resourced, more generally, SMEs lack awareness regarding the Y2K impact, resources, and the technical know-how for fixing the problems. Given the time constraints, there is very little chance of changing that reality. The best we can do now is try to increase awareness, provide easy-to-use tools and accessible resources, and provide attractive incentives for Y2K compliance efforts. The only hope is that the SMEs, as well as other organizations who are coming into the game late, can take advantage of the work done by others. In this context, it should be mentioned that the new federal law designed to encourage disclosure of information has not yet yielded the desired results.[3] It is quite clear that additional work needs to be done to provide increased incentives for information sharing. This is an area where intervention and action by the federal government can yield positive and fruitful results.

Control and Instrumentation Vendors

The major control and instrumentation vendors canvassed in this study are involved in an extensive program to provide Y2K compliance for their products. There is, however, reason to believe that some independent control systems integrators may have developed and implemented control systems for which there is little or no paper trail. In addition, some vendors are no longer in business, and some are not as cooperative as the major control and instrumentation vendors. One area of concern is the small vendors and system integrators who may have done very little to test and certify their products. These system integrators will have difficulty in responding to the calls from their clients. In addition, many of these vendors and system integrators are not aware of the Year 2000 Information and Readiness Disclosure Act designed to promote information exchanges.

Y2K Awareness

Awareness about the Y2K problem and the potential impact on control and instrumentation systems is high in multinational companies. However, there is considerable variation in terms of remedial response programs. In comparison, Y2K awareness is relatively minimal at SMEs.

As mentioned earlier, most of the large and multinational companies are aware of the threat, know where to look for information, and have the know-how and resources to develop and implement compliance plans. Beyond that, awareness about the Y2K threat falls off very rapidly. The need for awareness can be categorized into the following areas:

- Basic awareness of the threat,
- Awareness regarding sources of information,
- Awareness regarding devices or equipment that may fail,
- Awareness regarding federal regulation about information disclosures,
- Awareness regarding government incentives, such as EPA waiver of civil and criminal action for Y2K-related testing, and
- Awareness of contingency planning.

Risk Management Plans

Certain facilities are required to develop and implement risk management programs (RMProgram) by June 1999. The program, mandated by the Clean Air Act Amendments of 1990 and enforced by the EPA, regulates about 66,000 facilities. While all these facilities may potentially have Y2K problems, it is important to note that the total universe of Y2K-vulnerable facilities is much larger than the RMProgram facilities. Under the RMProgram, regulated facilities are required to conduct a hazard assessment, develop and implement a tiered prevention program, and implement an emergency response program. A brief summary of the RMProgram is included in Appendix VIII.

The hazard assessment includes development of worst-case and alternative release scenarios for the listed chemicals as well as compilation of 5-year accident history. It is important to point out that the worst-case and alternative release scenarios do not require

the identification of Y2K-related failures. For example, the worst-case scenario is by definition the "release of the largest quantity of the chemical taking into account operational and management controls."

The prevention programs are tiered based on the hazard assessment, the highest level being a parallel of the 14-element OSHA process safety management program. In addition, facilities must also implement an emergency response program and share information with local emergency response organizations as needed. Finally, regulated facilities must also compile a risk management plan (RMPlan) which consists of a description of the facility's RMProgram (i.e., the hazard assessment, the prevention program, and the emergency response program). The regulation also requires that the RMPlan be submitted to the EPA no later than June 21, 1999. EPA plans to make the RMPlan available to the public.

The intent of the RMProgram is to minimize the likelihood and consequences of catastrophic chemical releases. Thus, in principle, the activities and programs developed for compliance with the RMProgram should be beneficial for preventing Y2K-related catastrophic accidents. However, it is important to note that the RMProgram itself does not have any direct effect on the identification or correction of Y2K-related failures.

Another important consideration is that the RMPlans will be available in June 1999 when the general awareness about Y2K will be significantly elevated. It is quite likely that these two issues will be linked for facilities regulated through the RMProgram. Facilities should therefore expect public queries regarding their Y2K readiness.

Role of Federal Agencies

The federal strategy is to provide the public with candid information and assessments of Y2K compliance status[4]. Overreaction and panic occur when people have insufficient, inaccurate and irrelevant information and thereby assure that rumors hold sway. The federal government through President's Council on the Year 2000 Conversion and activities of different agencies is trying to encourage the following:

- Get pertinent and candid information out to the public,
- Demonstrate that organizations are managing against the problem,
- Establish that normal emergency response mechanisms have been reviewed and updated, and
- Share technical information via the Information Disclosure Act.

However, there are some practical problems regarding disclosures of technical information. For example, if a company discloses adverse information about Y2K compliance, does its market value go down? There are also issues regarding liability from lawsuits notwithstanding the federal "Good Samaritan" law.

Regulatory Approach and Development of Uniform Standards

Instituting new regulations to standardize testing or certification is not a reasonable approach for three reasons. First, in the remaining time, it is not possible to develop the mechanism and logistics needed for rulemaking, standard development, and establishment of reporting procedures. Second, implementation of any standardized method or regulation may cause penalties and unnecessary complications for many companies that do not fit the selected standard but have already expended an extensive amount of effort on Y2K compliance. Third, it is critical to minimize overall administrative efforts in order to focus available resources on the remedial efforts within this limited time frame.

Many experts and agencies do not believe that a regulatory approach is a viable alternative. For example, to compel submission of certification of Y2K compliance to EPA, absent a congressional mandate that directs reporting EPA would have to initiate rulemaking action. This rulemaking action would invoke all of the notice and comment procedures mandated by regulatory statute and other administrative law. Even if EPA suggested voluntary submission to certify Y2K compliance, provisions of the Paperwork Reduction Act, which require a public notice and comment period, would still need to be satisfied. Presuming the regulatory and procedural issues could somehow be waived, it is

unclear what action EPA or any other regulatory agency could manage receipt of certification documents from tens of thousands of companies, as only a very small number of trained staff exist to review and validate the submissions. Given the time frames required, it appears that the unmovable deadlines imposed by Y2K prevent regulatory approaches from being viable options to recommend to the U.S. Congress.

Any form of Y2K relief and remediation legislation should also be carefully crafted, particularly at this late date. For example, a law that is currently being proposed before the Texas legislature creates an incentive for all makers and users of Y2K devices to identify and implement remedies, by providing protection from liability from lawsuits [5]. Some interpret this proposal as fairly easy for manufacturers to meet the requirements for protection under the law while it would be very difficult for users to achieve the same level of protection. As a result, if Y2K failures generate many lawsuits, it is possible under this proposal that the companies who created the problem would be protected while their customers (particularly the least sophisticated) would remain liable. Also, it is not clear if legislation or new standards will be able to eliminate the exposure from Y2K-related failures at SMEs.

EPA Activities

The President's Council on the Year 2000 looks to EPA as the agency to lead the outreach effort for Y2K in the chemical industry.

The EPA is providing Y2K-related information through its website and other communication media. Also the Chemical Emergency Preparedness and Prevention Office of the EPA issued a Safety Alert in February 1999. In addition, Y2K information will be distributed with RMP materials emphasizing the Y2K issue and prevention of accidental releases that may harm workers, the public, and the environment. Also, EPA believes that RMP information may be an opportunity for companies to voluntarily communicate to the public what they might be doing relative to Y2K.

Under the General Duty Clause of the Clean Air Act (CAA section 112(r)), owners and operators of facilities with hazardous substances have a general duty to prevent and mitigate accidental releases. EPA believes that facilities have a responsibility to address potential problems due to the Y2K change as a part of this general duty requirement.

EPA's Office of Enforcement is also trying to encourage testing through the Y2K enforcement policy.[6] Under this policy, EPA states that its intent is to waive 100% of the civil penalties that might otherwise apply, and to recommend against criminal prosecution, for environmental violations caused during specific tests that are designed to identify and eliminate Y2K-related malfunctions. This policy is limited to testing-related violations disclosed to EPA by February 1, 2000, and is subject to certain conditions, such as the need to design and conduct the tests for the shortest period of time necessary, the need to correct any testing-related violations immediately, and other conditions to ensure that protection of human health and the environment is not compromised.

OSHA Activities

OSHA is providing Y2K-related information through its website and other communication media. OSHA has further suggested that the agency will help through a compliance assistance approach that involves outreach and educational materials, speeches, and the continued use of OSHA's website to disseminate information about the Y2K problem[7]. OSHA also has preliminary plans to sponsor a Y2K Web Forum to further highlight and address the problem, and has a project to send letters to employers calling their attention to the issue as part of a larger outreach and communications plan. In addition, upon inspection, OSHA compliance officers now distribute Y2K fact sheets to employers. Finally, OSHA is discussing ways to obtain the support of the 50 OSHA State Consultation Programs to assist in the Y2K outreach efforts.

OSHA, however, does not expect to invoke the General Duty Clause (Sec. 5(a)(1)) of the Occupational Safety and Health Act to compel compliance in firms where potential for accidental

release exists because of unforeseen microprocessor failure. The General Duty Clause can only be used after certain stringent legal tests have been satisfied. These legal requirements include documentation that employees are actually exposed to a hazard, that the hazard is serious, that the employer recognizes that the hazard exists, and that there are feasible and existing methods of controlling or abating the hazard. Especially in SMEs, where Y2K awareness is relatively very low, it may prove difficult for OSHA to prove these elements in order to invoke the General Duty Clause.

Companies have a responsibility under OSHA's Process Safety Management rule to ensure that potential hazards associated with equipment which can affect the integrity of a covered process and which might be affected by the Y2K problem, are properly managed. OSHA's 14-element process safety management program (29 CFR 1910.119), mandated by the Clean Air Act Amendments of 1990, is an industry practice that where effectively applied can help prevent many of the Y2K-related problems. The 14 elements of the program are:

Employee participation	Pre-startup safety review
Process safety information	Hot work permit
Process hazards analysis	Emergency response plan
Operating procedures	Incident investigation
Training	Contractors
Mechanical integrity	Compliance audit
Management of change	Trade secrets

For example, under the process safety management program, facilities conduct Process Hazards Analyses (PHAs), such as Hazard and Operability (HAZOP) Studies and Management of Change Analyses (MOCs) to identify failure scenarios and the resulting consequences. Even though facilities have not traditionally considered Y2K-triggered failures, it stands to reason that a thorough PHA and MOC would have considered the secondary failure (e.g., power failure, loss of cooling water, malfunctioning of a pump) triggered by the Y2K failure. Additionally, other elements of the process safety management program (e.g., mechanical integrity, emergency response program, operating procedures, etc.) should provide a higher

degree of reliability for the facility. In contrast to the new EPA RMProgram, OSHA's process safety management program has been in place since 1992. It may be inferred that the systems and procedures in place have gone through significant continuous improvement, and thus may reduce the possibility of catastrophic accidents caused by Y2K-triggerred failures. However, similar to the EPA RMProgram, the application of the process safety management program is also quite limited in scope, and does not include all the Y2K-vulnerable facilities.

International Efforts

On the international front, the Organization for Economic Cooperation and Development (OECD) issued a major press announcement as a result of their December meeting on chemical accidents. OECD has also established a Y2K-related website that addresses some of the specific Y2K issues.[8] Another international organization called the Intergovernmental Forum on Chemical Safety (IFCS) has also issued an international alert on Y2K.[9] IFCS is also seeking an Internet communication vehicle that might provide information to more parties, particularly those in lesser-developed countries, which may have industrial facilities facing the same kinds of Y2K hazards.

State and Local Agency Activities

State and local governments are providing varying levels of Y2K information, resources, and support. For example, Washtenaw County (a mixed urban and rural area located in southeast Michigan) has been investigating and correcting, when possible, particular Y2K issues[10]. However, the Y2K issues that involve working within the community pose problems more complex and not so easily solved. For example, how are facilities communicating their Y2K contingency plans to local agencies, the local emergency planning committees, and the residents in nearby communities?

In short, even though constrained by limited resources, local governments and state agencies that are aware of the potential of Y2K problems are willing to play a significant role in working with the facilities. However, these efforts could be improved

significantly with federal leadership, attention, and resources. The main problem is that in many cases these local and state governments are oblivious of the threat. In the limited research conducted for this study, the following information was identified[11]:

- According to a survey by the National Association of Counties announced on 12/8/98, half of the county governments lack a plan to deal with Y2K preparedness, contingency planning and emergency response.[12] This will impact the potential availability of emergency response services, 911 communications, and sewer and water treatment systems.

- According to a survey by the Emergency Response Research Institute, released on 12/4/98, less than a third of the emergency response organizations surveyed have begun Y2K contingency planning activities, and less than a quarter have looked at the external effects of other organizations' Y2K compliance on their ability to provide emergency response services.[13]

The Year 2000 Technology Problem

The Year 2000 Technology Problem, also known as the "Y2K Problem" or the "Millennium Bug", stems primarily from a simple two-digit year representation. In the early days of computing, computer memory limitations caused programmers to represent years in a two-digit format – for example, "99" instead of "1999." This practice became standard for the computer technology, both for software as well as embedded microchips. The microchips, numbered in billions, are embedded in almost everything we use today. The Gartner Group estimates about 50 billion microchips in embedded systems worldwide and about 1 percent of these microchips will have Y2K-related failures leading to shutdowns, erroneous results, and chaotic behavior[14]. Of this, a fraction is involved with mission-critical systems, leaving on the order of 25 million microchips (deployed in systems) which must be repaired worldwide in all sectors of the economy.

The chemical process industry relies on software and microchips for the operation, maintenance, and control activities that are vital to the safe operation of the plants as well as the profitable manufacture and distribution of chemical products. Software or microchips that store dates as two digits could render incorrect results. For example, a control device may have been programmed to provide a reading or report every six months using the two-digit arithmetic. Such a device could interpret the year 2000 as "00" and calculate a negative number when measuring time intervals. The outcome of such an event could pose a problem. The question is: would the computer ignore the incorrect answer, or could it cause the hardware to malfunction, or cause a major process upset?

Other such date-programming or date-embedded problems can be categorized as follows:

- Dates stored as two-digits may assume the year 1900 instead of the year 2000;
- 00 may not be allowed as a valid date;
- Dates may be required to begin with 19;
- Dates may have assumed a range that ends in 1999;
- Reports may assume and print a 19 as the first two digits of the year;

- Dates such as 9/9/99 may cause hardware and software problems;
- Leap year may be incorrectly calculated for the Year 2000, resulting in problems around February 29, 2000 and December 31, 2000 on the 366th day of the year.

Potential for Catastrophic Events Stemming from Year 2000 Non-Compliance

The potential for catastrophic events stemming from Year 2000 Non-Compliance can be divided into three categories. First, failures in software or embedded microchips within the process plants may cause process excursions or control problems resulting in accidents. Second, external Y2K-related problems, such as power outages may cause various problems, such as accelerated shutdown of processing, monitoring, and safety systems. Accelerated shutdowns may cause other problems such as the triggering of fire suppression systems, causing loss of water pressure for actual fires, and disabling such systems. Third, multiple Y2K-related incidents may exceed the capacity of emergency response organizations to respond.

Other factors that must be considered are applications that are purchased from a supplier and customer applications that are developed by the users. In addition, the current utilization of integrated operations using multiple applications all of which pass on information/data, or use information/data makes it mandatory that users consider this in their readiness and operational contingency plans.

Failures in Software or Embedded Microchips

The chemical process industries, irrespective of size and type of operations, use a variety of software and embedded microchips to operate, maintain, and control their processes. Y2K-related failures, can at the minimum, cause off-specification products or shutdown of the process and at the extreme cause process malfunctions leading to accidents. For example, the agitator on a batch reactor may fail to operate causing the initiation of a runaway reaction. The emergency shutdown system (ESD) is expected to stop the runaway reaction but the ESD itself may have an embedded chip that may be susceptible to Y2K-related failure.

Many other examples exist for both batch processes as well as continuous processes used by the chemical process industries.[15]

Chemical processes are usually built with multiple layers of safeguards that require the congruent failure of various systems to precipitate an accident. However, many accidents in the U.S. and overseas have occurred when multiple simultaneous failures resulted in catastrophic accidents. In addition, some automated safeguard systems are "on-demand" or "in reserve", making recognition of the potential for failure very difficult. Thus, it is prudent to explore the catastrophic potential of single Y2K-related failures as well as combinations of various failures.

Power Outages

No effort was made in this study to assess the potential of power outages from Y2K-related failures. However, potential Y2K-related power outages represent another set of problems for chemical and petroleum facilities. While many chemical and petroleum manufacturing facilities have backup power generators, Y2K failures may include concurrent loss of power, cooling water and other system malfunctions. First, plants without auxiliary power backup systems face a threat to parts of their processes that may not shutdown in a fail-safe mode. Batch chemical processes are especially susceptible because the safety of the process is quite often dependent on time-dependent factors such as precisely timed mixing, heating or cooling requirements. Second, a potential scenario is that widespread power outages may cause shutdowns of many plants, which in turn will require simultaneous startups. Although startups of chemical plants are infrequent and their durations are short compared with the life cycle of a plant, process safety incidents occur five times as often during startup as they do during normal operations[16]. Thus, a large number of simultaneous startups may increase the potential of incidents in one or more process plants. In addition, the simultaneous restarts of large power-consuming facilities will impose large demands on the electrical grid.

Emergency Response

Similar to power outages, no effort was made in this study to assess the impact of Y2K-related failures on emergency response organizations themselves, nor were there assessments of the larger social ramifications of Y2K failures. It is reasonable to assume that response organizations may also have Y2K-related issues which should be explored separately. For example, response capability will be impacted by loss of power, failures in communications (telephone, radio, TV, and computer telecommunications) and compromised home situations for professional and volunteer responders. However, even under the best of circumstances where the emergency response organizations continue to operate without any major problem, multiple incidents could strain the resources and effectiveness of the system. Over extended emergency responders and mutual aid organizations may be unable to respond in a timely manner.

The Extent of the Problem

There is no doubt that the impact of the Y2K problem is one of major proportion. Various estimates, ranging from millions of embedded microchips to billions of lines of software programming, are quoted by different sources. However, there is quite a bit of disagreement on the potential outcome. Some participants at the Technical Workshop convened for this study claimed that they could not identify a single catastrophic failure that could be attributed to Y2K-related events. On the other hand, some of the other participants were quite persuasive in their argument that because of the underlying causes discussed below, there is a reasonable potential for major accidents. All participants were unanimous that the main exposure might result from Y2K non-compliance in small and mid-sized enterprises (SMEs). For the purposes, of this report, SMEs are defined to include following types of facilities: facilities that have less than 50 employees, Facilities that have between 51-200 employees and are not part of a multinational national corporation, or Public sector facilities, e.g., municipal water and wastewater facilities

Definition of Y2K Compliance

Even though there is significant disagreement on the extent of the Y2K problem, there is unanimous agreement that the prudent approach is to take preventative measures.[17] In general, this means a Year 2000 compliance program. However, there is quite a bit of

disagreement as to what compliance means. In the absence of specific regulatory framework to assess compliance, it follows that established standards for testing and certification do not exist either. Presented below is a compliance approach that is being implemented by some of the companies contacted during this study. It includes four basic steps:

- Inventory,
- Assessment,
- Remediation, and
- Testing and Certification.

Inventory includes compilation of inventory of all hardware/software systems that are susceptible to Y2K failure. For process industries, this could mean complete control systems, pumps, compressors, automated agitators, and a host of other devices and equipment[18]. An example checklist for a plant is provided in Appendix IV.

The assessment step (which may include some preliminary testing) requires an analysis to determine if the system (large or small) is safety-critical; could an individual failure or failure in combination with other systems result in a process safety incident. The assessment step is quite similar to a process hazard analysis conducted by process plants. A classic hazard analysis approach for finding Y2K-related safety-critical problems is to answer three basic questions:

- What will happen if this system fails because of a Y2K problem?
- Will a Y2K problem occur in this system? What are the plausible failure modes?
- Will the consequences be severe enough to cause any concerns?

The remediation step requires fixing or replacement of safety-critical systems identified in the assessment step.

Testing and certification is the final step that ensures Y2K compliance using accepted industry standards. Vendors and other

organizations have made available testing and certification standards. Some are also providing services for testing and certification of different devices. The testing includes integrated testing across several devices, and not just the evaluation of individual devices. Also, it is important to conduct realistic testing, assuming realistic or simulated actual conditions. For example, embedded microchips manufactured by the same vendor may respond differently based on how they are configured in the system. Thus, it is necessary to test the integrated systems and implications of those systems as well as the microchips themselves.

Operational Aspects of Y2K in Chemical Plants

There is no central clearinghouse which has compiled the Y2K findings, remediation plans, and contingency plans for the U.S. chemical process industry. Yet there is little doubt that all companies, from multinational giants to SMEs, have the potential to be affected by Y2K-related failures. Although detailed chemical operating company information is not available, many companies discuss the issue on their web sites.

The Securities and Exchange Commission requires that a public company disclose its Year 2000 status in its Management Discussion and Analysis (MD&A) sections of annual and quarterly reports if: 1. Y2K readiness is not evident as demonstrated by completed testing and assessment of third party issues, and 2. Management believes that the consequences of its Year 2000 issues would materially affect the firm's business.[19] The MD&A disclosure requires description of the firm's readiness for both information technology systems and non-information technology (embedded) systems, costs for addressing the Y2K issues, risks (worst-case scenarios), and contingency plans.

More extensive information is available from the Securities and Exchange Commission "Edgar" database. The Management Discussion and Analysis (MD&A) of Financial Condition and Results of Operation section of companies' disclosure documents usually provide more information than the web sites. The cost estimates for Y2K remediation given in these MD&A sections leave no doubt that operating companies are serious about Y2K. Some of these cost estimates are given below for various companies:

Dow Chemical	$50,000,000 to $70,000,000
Dixie Group	$400,000
DuPont	$300,000,000 to $400,000,000
Chemfirst	$12,000,000
Engelhard Corp.	$14,200,000,
Ethyl Corp.	$2,70,000 to $2,800,000
Exxon Corp.	$250,000,000 to $270,000,000
Nalco Chemical Co.	$3,000,000
Shell Oil	$150,000,000
Sunoco	$36,000,000
Union Carbide	$50,000,000 to $60,000,000

Essentially all companies are funding Y2K modifications through their operating budget or by reallocation of other funds. In addition to these sources of information, the Chemical Manufacturers Association (CMA) is in the process of surveying the CMA members in order to provide information on "do we know how well our members are doing to meet the Y2K challenge?" The survey is being conducted so that the information is not traceable to an individual company. The results of the survey were not available at the time of the publication of this report. The American Petroleum Institute (API) has a Y2K task force that meets every 6 to 7 weeks. The meetings are open to non-API members. However, some information such as API's Y2K testing database is free only to API members (and available at a nominal fee to those that are not API members). The Chlorine Institute has a web page where members are able to share Y2K information. The Chemical Information Technology Association has a Year 2000 Subgroup which meets quarterly and interacts continuously with the exchange of Y2K program information and results of mutual value.

From the chemical process plant perspective, two issues must be addressed: plant operations and contingency planning. Specifically, what can be done to insure safe and continuous chemical process plant operations and how to assure that the contingency plan is adequate enough to prevent the Y2K failures from creating undesirable consequences? Occidental Chemical[20] and Rohm and Haas[21] provided brief presentations (included in Appendices IV and V respectively) of their Y2K compliance

efforts.[22] The following discussions on plant operations and contingency planning are gleaned from the Occidental Chemical and Rohm and Haas presentations, as well as discussions during the Y2K Technical Workshop, and other research conducted during this study.

The five key areas that corporate Y2K compliance programs in multinational companies are focused on:

- Information Technology,
- Chemical Process Control Systems,
- Suppliers,
- Customers, and
- Contingency Planning.

Each area of the Y2K program depends on a process that includes the following steps:

Inventory - identification of all the devices, systems or relationships where there is concern about Y2K failures.

Investigation - determining the true likelihood of failure and the impact should failure occur.

Remediation - actions that will correct the Y2K related deficiency or mitigate the impact of a failure.

Documentation - creation of information needed to share results and show due diligence.

Of the five key areas listed above, the two areas that have a potential impact on chemical process safety are:

Control Systems - to identify and correct the problems associated with microprocessors and programming that is embedded in systems and devices used to monitor and control chemical process plants.

Contingency Planning - to identify the likely scenario of Y2K failure and make plans to address it, and to identify possible situations and ensure ability to respond to them.

Plant Operations

Chemical process operations are heavily dependent on control systems, predominately automated process control systems. These systems consist of field instrumentation, which often contain microprocessors, in addition to the programmable logic controllers (PLC) or distributed control system (DCS) that are used as the 'brains' of the automated system. When a PLC or DCS is not able to maintain control of the process unit, safety interlocks are utilized to bring the plant to a safe state, regardless of anything else going on in the plant. These safety interlocks may utilize either hard-wired (relay) or PLC based systems to define the actions taken when the specific process variable reaches its defined "out of control" set point. Y2K compliance programs for chemical process control systems consist of the following steps:

Inventory

- Identify all systems and devices containing microprocessors and programming.
- Prioritize all identified items according to both likelihood of failure and potential impact should a failure occur.

Investigate

- Develop enterprise-wide standard methods for investigating devices.
- Eliminate items with low likelihood of failure and low impact based on the priorities established in the inventory step.
- Eliminate items screened elsewhere, from consideration for further efforts, based on corporate shared information. Developing corporate databases containing the information about devices that have been investigated at each facility can facilitate this.
- Based on vendor and corporate information, eliminate items that have been tested and confirmed to be compliant or

considered not to be a Y2K device from consideration for further efforts.

- Based on physical inspections, eliminate devices that are not Y2K devices from consideration for further efforts. For example, examination of an instrument specification sheet may indicate that it does not require battery backup; neither can it maintain an internal date and thus it is not a Y2K device. Also, physical inspection also may indicate that the device can exchange only analog signals (as compared to digital signals), thereby demonstrating that it is not a Y2K device. If these simpler and less expensive methods fail, more rigorous preparation and execution is employed for detailed testing.
- All the inventory and assessment information is compiled in a database and shared throughout the corporation. The database is designed with the broader communication goal in mind. For example, unique spreadsheets with differing categories of inventories and assessments from each separate facility would not be very useful.

During the investigation step, it is important not to spend all the time working on the "means to the end". The best course of action is to identify, assess, and remediate problems as quickly as possible. While not a particularly demanding issue, there are some important subtleties about Y2K. For example, the clock cycle issue, e.g., the issue of register overflow. An untrained technician may not perceive that a device uses a date and may observe that it does not print a date. However, does not guarantee that somewhere in the device a date is not being used, is not critical and may not cause a Y2K failure. Another critical factor is that some Y2K failures may not occur in the year 2000[23]; thus it is important to integrate Y2K thinking into everyday business.

Remediate

- Create standard methods so that the methods can be used throughout the enterprise. The standard methods should focus on remediating the Y2K problem only. Otherwise, if the Y2K compliance effort is used as an opportunity to fix other problems, it may result in too much time and capital expended

on re-engineering such that the Y2K problem is not fixed in time.
- Take advantage of the patches and fixes supplied by vendors to make the remediation effort significantly easier. However, when a facility's Y2K team member discovers that a vendor does not appear to have a plan for assessing and testing their devices, the situation is pursued on an accelerated basis at a higher corporate level.
- Track the remediation to ensure closure and after closure use appropriate methods to test the device.

Document

- Create a minimum standard for documentation. The standard takes into account What, Who, Where, and When regarding compliance efforts.
- Create Y2K compliance documentation for each device using established standards. Duplication of the documents at the plant and the corporate office is avoided by using a standardized documentation system.
- While the Y2K compliance effort is ongoing, conduct audits to ensure that established processes, standards, and methods are being followed.

Some of the findings and conclusions reached by multinational companies during their Y2K compliance efforts are given below:

- Surveys of Y2K efforts among larger corporations canvassed and researched during this study indicated that single device failures caused by the Y2K problem are unlikely to result in catastrophic chemical releases. However, it is unclear what the outcome might be from multiple failures, e.g., multiple control system failures, multiple utility failures, or a combination of multiple utility and control system failures. Multiple failure possibilities are not considered in current process hazard analyses.
- One company reported finding about a 7% remediation need, primarily replacement of computers. Even for big companies, the number of problems, while not major as individual problems, is significant. However, the outcome of the

combination of these individual problems along with utility and other contingency problems varies. For example, the outcome may be quite different if the electrical utility has a 90% chance of survival as compared to a 10% chance of survival.

- In one case, a consultant team identified 10 times as many Y2K issues as did internal auditors. However, it should be pointed out that the facility in this case was in the earliest phase of the inventory process. In other cases, where the facility is well into its inventory process, discrepancies may not be that significant.
- There is extraordinary interdependency involving a facility and its external suppliers and customers. However, entities should concentrate on problems they can solve. They should not be overwhelmed because they can not answer questions on every external influence.
- Central coordination is necessary.
- Corporations are sharing information between companies and entities, with whom they have a business relationship or association.
- The greatest threats are utility failures and multiple-concurrent failures. Redundant systems with the same Y2K failure problems will fail redundantly.
- In some instances, as much as 3% of vendor information was incorrect.
- Some corporations are planning to shut down operations through the millennium transition. It is planned that their plants will be idle but staffed during the transition. (It should be pointed out that most of the processes for these corporations are batch processes and usually do not produce chemicals on New Year's Eve.) Because of higher financial costs and other safety considerations, continuously operating plants are less likely to shut down. However, many are evaluating contingency plans taking into consideration safety, utility continuity, supply reliability, and customer needs.
- Global corporations should take advantage of year-end process performance information as midnight marches around the world, starting in the Pacific rim and moving westward through Asia, Europe, and finally the U.S..

Contingency Planning

Contingency planning consists of evaluating the worst-case scenarios and then developing response plans for those scenarios. The General Accounting Office has developed guidance for Business Continuity and Contingency Planning that articulates the general principles that all businesses should consider when making a contingency plan.[24] Existing plans, such as Emergency Response Plans, Business Continuity Plans, and Disaster Recovery Plans, provide an initial basis to help develop the Y2K plan. However, Y2K contingency planning differs from normal disaster planning by anticipating potential problems may happen simultaneously and in several places at the facility.

The Worst-Case Scenario

The Securities and Exchange Commission (SEC) requirement for a worst-case scenario is prudent, since it tends to focus each plant and each company on truly understanding what is the worst-case. The SEC requires the facility to look at the Information Technology Systems, Control Systems and Safeguards, Suppliers, close-linked Customers, and the Surrounding Community and determine the worst-case scenario for each category. Based on these analyses, a composite scenario is created that assumes multiple problems occurring simultaneously. These scenarios can also be developed by conducting process hazards analyses, such as "What-If" exercises and "Table-Top" exercises. Since the New Year occurs in the middle of winter, weather should be considered in the contingency plan development, particularly for facilities subject to extreme freezing temperatures and precipitation in the form of ice, sleet and snow.

Emergency Response Planning

Preparing for emergency response requires the identification of unlikely situations and unrecognized situations. This allows the facility to determine the areas where resources, personnel and attention needs to be focused. During these analyses, it is important to determine the impact of failure of equipment and systems that are usually taken for granted. The process leads to the identification of new systems that need to be addressed. Thus contingency planning includes failure of utility systems and control

systems, as well as the potential for unanticipated, newly recognized Y2K-sensitive devices and components to fail. The final step is testing of emergency response capacities in addressing these situations.

Contingency planning must also take into account human factors issues regarding appropriate staffing, appropriate hours of continuous work and rest intervals, and worker stress levels. Worker input should be sought in the design of contingency plans and workers should be trained on the contingency plans. In addition, workers and emergency responders can do their job effectively if they have assurances that their families are safe and are not being impacted by any other emergencies in their home community.

Contingency planning for Y2K-related emergencies is categorized into three broad groupings. Contingency planning for continued safe operations, safe shutdown, and then finally emergency response:

Contingency Level 1: Continued Safe Operations

The first level of contingency planning addresses those operations that are necessary to keep the facility running in a safe and environmentally sound manner. This includes pre-planning of actions that can be taken to allow the facility to continue to run in a safe and environmentally sound manner, even if the Y2K compliance efforts fail to prevent a Y2K-related failure. With all these additional activities resource training and refresher training must be addressed, not just a one time effort but something sustained that insures operations people are fully oriented and qualified to implement these alternative strategies and operational activities. The important issue is whether operators will be able to recognize operational problems, and be able to respond quickly and correctly to what they recognize from the indications from their control room CRTs. Examples of activities that can be categorized under Contingency Level 1 are given below:

- Minimize finished product inventories and waste effluent levels to allow as much reaction time as possible to address unusual situations

- Maximize raw material inventories (within safe limits) in case a supplier fails (Note: In addition to limitations imposed by the transportation system, this action may create problems with facility siting issues, and should be addressed through process hazard analyses)
- If facility operations depend upon a small steam supply source, consider renting a backup mobile steam generator in case the supplier fails
- Consider using bottled gas and/or portable compressors for air and nitrogen backup
- Consider using low-tech/cheap radios to backup sophisticated communication systems
- Increase Operations and Craftsman personnel staffing during critical periods in order to respond quickly to unusual situations
- Shutdown non-essential units; restart them after critical times have passed and essential units are running well
- Make pre-arrangements with alternate transportation sources to handle material if primary transportation modes are not available
- Develop a plan to manually control output from normally automatic controllers (switch to fixed speed and control volume output via dampers, valves, etc.)
- Identify and test manual overrides for security and safety systems

Contingency Level 2: Safe Shutdown

Contingency level 2 is activated if the activities described in contingency level 1 do not work. Since continued safe operations are not possible, the facility must consider safe shutdown. This contingency level planning includes ensuring the availability of all personnel, equipment, utilities, services, and other resources needed to ensure safe shutdown. These issues or items could arise from something overlooked at the site or it may also be caused by an external influence. Shutdown systems and other devices that ensure safe shutdown are tested as part of the contingency planning process. Examples of activities that are covered under Contingency Level 2 follow:

- Rent portable electric generators or lights for emergency use
- Increase operations and craftsman staffing during critical periods to monitor and react quickly for shutdown purposes
- Shutdown non essential equipment before critical periods to allow more attention time for shutdown of critical systems
- Ensure all emergency shutdown equipment and safety systems are fully functional before critical periods (test them)
- Test Uninterruptible Power Supply (UPS) and other backup systems to ensure power is supplied to control systems for safe shutdown
- Consider having a backup low/tech radio system for use if the main system fails
- Pre-test emergency vent scrubbing systems to eliminate or minimize emissions during shutdown
- Conduct Shutdown Drills -- consider more than one system failure and limited access to external resources
- Alert the emergency response community
- Alert utilities whenever shut down will result in a significant change in the demand.

Contingency Level 3: Emergency Response

Contingency Level 3 is activated when contingencies in level 1 fail to ensure continued safe operation followed by failure of contingencies in level 2 to ensure safe shutdown. This may indicate the initiation of a process safety incident. Thus planning for contingency level 3 requires that things necessary for an adequate and proper emergency response to Y2K-precipitated incidents are available. Examples of activities that are included in Contingency Level 3 are given below:

- Consider having the Plant Emergency Response Team on stand-by at the facility
- Work with "outside" responders and pre-plan a backup communication mechanism and practice a response plan
- Develop a system to alert neighbors in case the local emergency warning system fails
- Conduct drills considering multiple system failures
- Within the facility
- With "outside" response agencies

Overall Operational Issues and Some Generic Conclusions

There is no question that large companies are taking the Y2K problem seriously and are expending a large amount of resources on the problem. These companies have concerns about the reliability of their utility supplies since they have no control over them. There must be trust and communication between all stakeholders and every entity must do their part.

Of major concern are small and mid-sized enterprises (SMEs). Individual SMEs were not present at the Y2K Technical Workshop, but vendors, consultants, and association leaders with expert knowledge of SMEs were present.[25] Based on their input, it is reasonable to conclude that in these companies the level of Y2K compliance efforts are not proportionately comparable to those in larger companies. In the little time left, there is very little chance of changing that reality.

The Y2K problem is a worldwide issue. Some insight may be gained from a Dutch survey of some 205 establishments that have reporting requirements similar to the U.S. Risk Management Program regulation.[26] It should be pointed out here that there is no comparable effort underway or planned at this time in the U.S..

Of the 205 establishments surveyed by the Dutch Health and Safety Inspectorate, 176 responded and the surveyors concluded that a reliable picture of the companies' approach to the Y2K problem could be drawn. All but three companies are surveying their hardware and software to determine if they are millennium-proof. The three companies not conducting a survey were said to have an explanation for not doing so. They had determined that they did not have any components or equipment that were vulnerable to Y2K problems.

The same Dutch survey also concluded that three-quarters of the operators are doing contingency planning in case something goes wrong. A number of establishments plan to shutdown their entire production process around the date change. Additional personnel will be brought in at a number of establishments. The survey revealed that there are 40 companies where problems may occur with the process control system or parts thereof. One control

system was found which could not handle the year 1999. Other areas where problems have been found include: measuring instruments connected to a control system, independent safety systems, telecommunications systems, access control systems and climate control for computer rooms. A majority of the respondents claimed that sufficient funds and manpower have been made available to resolve the problems. For 42% of the establishments, respondents believe that the major problems will have been resolved in 1998. The remaining 58% expect to have the problems resolved in 1999. In 94% of the companies surveyed, a project leader has been assigned and a project-based approach is being taken to find and solve the problems.

Process Controls and Other Equipment Issues of Y2K

The Y2K problem requires a balanced response from chemical and petroleum facilities, process control vendors, and other physical equipment suppliers. Most process control system vendors have been hard at work for eight months to more than two years on the Y2K problem as it affects their products. Major vendors are communicating with their customers directly via their sales force or representatives and via mail; however, the major communication means is via their web sites. Many of their web sites (See Appendix VI) address specific products and their Y2K compliance. Most vendors have a corporate policy regarding Y2K issues, and have an assigned person in charge of Y2K issues at the corporate level.

Process Controls

Process Controls are used in a wide variety of applications in the hazardous chemicals industries.[27] While the overwhelming majority of control systems continue to function with the date change, occasional problems are encountered. Mr. Dan Daley, Maintenance Director of Occidental Chemical, said, “we have found situations, and there are situations with some of the older operator consoles for DCSs that effectively will go to black screen.” Mr. Jordan Corn, Rohm and Haas, stated, “to date, we have found only one catastrophic control system failure, and let me qualify that a bit. Catastrophic meaning that the control system itself went to an unpredictable state from which you could not recover. The process could still have been shutdown safely, but

the control system itself was rendered completely inoperative." Prepared facilities anticipating such situations should manage the problems well. However, the certainty of safety at unprepared facilities is unassured.

Control system vendors were represented at the Y2K workshop by Bob Newell, Year 2000 Program Manager, Honeywell Industrial Control Division; Dave Hart, Y2K Issues, Rockwell Automation; and Dr. Angela Summers, Director of Premier Consulting and Engineering, Triconex Corporation. They provided input regarding their interactions with customers concerning Y2K issues.

Mr. Hart, Mr. Newell and Dr. Summers expressed concern that any mishap on January 1, 2000 may be perceived as a Y2K problem whether it is or not. If they are swamped with calls, how do they prioritize them? Vendors also need contingency plans for handling inquiries from their customers.

One vendor initiated a Y2K program in the fourth quarter of 1995, according to their disclosure statement.[28] "This program addresses the company's information technology systems and other systems with embedded computer technology; products provided to customers; products purchased from suppliers; and most recently, the year 2000 readiness of its significant customers." Almost all of their current products have been tested internally to ascertain if they are year 2000 ready. Approximately 99% of these products are year 2000 ready and the remainder are expected to be so by the end of January 1999.

Furthermore, the vendor formally communicates with customers to make them aware of any potential problems that may result from the use of older products that are still in use by their customers and subject to warranties or service contracts that may not be year 2000 ready. "The company expects to complete this process by the end of 1998. For older products which are not year 2000 ready, but are no longer under warranty or service contracts, various means are being employed to raise the awareness of any potential year 2000 problems, including advertising and contracting with external service providers to help identify current owners." This vendor also provides a comprehensive Product Readiness Matrix on the World Wide Web accessible though an online user registration.[29]

Another company lists their products by category[30] on the World Wide Web. A Date/Time Test Plan Template is also provided[31] describing the test procedure and documentation.

A third company began its Year 2000 testing in the spring of 1996.[32] They used the following sources to guide their efforts:

The Year 2000 And 2-Digit Dates:
A Guide For Planning And Implementation, fifth edition-IBM
Title: The Year 2000 and 2-Digit Dates: Guide – Vol. 1
Document Number: GC28-1251-07
Build Date: 09/12/97 16:00:09 Build Version: 1.3.0
http://www.s390.ibm.com/ftp/os390/year2000/y2kpaper.pdf

British Standards on Year 2000
The British Standards web page can be found at:
http://www.bsi.org.uk/disc/year2000/2000.html

Though they have identified some problem issues regarding Y2K compliance, these issues do not impair control of the process or loss of view of the process.[33] Approximately 90% of their Chemical Processing Industry (CPI) customers have at least begun addressing the Y2K issue, although some large companies are not totally engaged and a few small/medium companies have not taken any action. Most of their customers enrolled in their system revision service receive automatic upgrades.

Another vendor source indicated that pharmaceutical companies are all engaged and well ahead of other industries, with power companies second, and chemical, pulp and paper, oil and gas following about equal to each other. The same vendor also reports excellent feedback from its customers, who say the vendor, has done the right thing in a proactive and honest environment regarding the Y2K issue. This vendor also uses its web site to provide information on its products for customers.[34]

Other Equipment Issues of Y2K

Internal Y2K Equipment Audits may miss some devices. Equipment with embedded microchips can encompass a diversity

of devices; some of, which may not be apparent, even to facility personnel with extensive experience. Mr. Daley stated, "…Then we brought in a couple of consultants and they were named as specialists in Y2K, and they did inventories. And we found in both plants that we did the pilots in, we found a 10:1 ratio. We found that they identified 10 times as many devices as we had identified."

Demonstrating Y2K Compliance by the vendor does not assure compliance in the chemical-manufacturing environment. An examination of the vendors test procedure and retesting data is necessary and prudent. In some cases, vendors are unable to assure compliance for equipment that does not operate according to original design configuration, and after having been subject to customer modifications.

Vendors' tests cannot cover explicitly every version of their hardware, software, and combinations thereof. This is another argument for user testing. But, in addressing Y2K issues, companies must guard against getting involved in major new capital projects because there is not enough time.

In addressing Y2K contingency plans, Dr. Angela Summers highlighted the importance of evaluating the readiness of consequence mitigation systems, such as fire suppression water systems, pressure relief valves, and flares. These systems may be called upon to function in the event of a Y2K related failures, yet many of these systems are not sized to handle the multiple failure scenarios that may occur due to Y2K.

A neutral clearinghouse of user compliance test results posted on the World Wide Web could help reduce the work load and time constraints. Explicit documentation of hardware version, software version, as well as test procedure and results would be required. In addition, critical systems should continue to be user tested, since even chip level differences could cause lack of Y2K compliance.

Conclusions and Findings

Small and Mid-Sized Enterprises (SMEs)

The Y2K Technical Workshop members were quite concerned about Y2K failures at SMEs. Multinational companies and other organizations may be willing to make available Y2K information and tools to SMEs. However, this willingness is tempered by concerns about legal liability to individual companies or trade associations that contribute the information. For example, if Y2K checklists or tools are made available through a website used by an SME, and yet that SME still has a Y2K problem for whatever reason, could the SME sue the information provider? This problem could be alleviated or eliminated completely by making the information available through a government agency. For example, Occidental Chemical and Rohm and Haas have identified, tested, and validated specific devices. These lists along with other appropriate checklists and compliance plans could be provided through a federal agency's website without mentioning company names and with appropriate cautions and suggestions regarding SME application.

SMEs have lesser access to associations such as API and CMA, which have helped corporate entities become educated on safety issues. An exception to this may be the propane distributors who have a well-developed organization that is engaged in dialogue with the government. Also, the Chlorine Institute is making Y2K information available through their website. The information that is being provided is quite generic and fragmented, and has not been assessed for its utility to SMEs. The experiences with some SMEs on other issues seems to indicate that in order to be useful, the information provided has to be very detailed and specific to the SMEs.

In addition, large businesses and even SMEs have restructured and thus have fewer resources to devote towards time limited technical problems. To compound the problem, trade associations have also undergone restructuring and as a result may not have the resources needed to serve their membership.

One approach to reach the SMEs may be to identify trade or professional organizations that serve most of the Y2K-vulnerable SMEs, and then work with these organizations to enable their membership to address Y2K problems. In order to be effective, it may be necessary to provide easy-to-use models. SMEs must be able to access concise and relevant information that they can apply very easily without having to expend extensive financial and human resources. Examples of useful information include: readiness plans, detailed checklists integrated with risk management functions, contingency planning tips, and checklists for communication and sharing of information with local responders. Developing a council of major chemical companies, suppliers, and governmental organizations to develop guidelines might be an excellent way of establishing "real content." Time is of the essence and this task must be done immediately.

Risk Management

Risk management generally consists of a variety of programs and activities to assess and manage risks. To be fully effective these programs must be implemented with the complete involvement of the management, labor, and local responders. Risk management also includes the utilization of best practices (e.g., equipment, procedures, auditing, testing, and certification), adherence to industrial and professional society standards, and compliance with applicable regulations. The chemical processing industry has practiced these risk management principles for a long time. It is quite apparent that the Y2K issue will test the existing system of safety, and failure may engender review of policy issues as well as review of industrial programs and practices.

There is a general consensus that facilities doing an effective job in managing their risks should not see any major problems. The logic is that the Y2K problem is another risk that has to be managed.

Utility Issues

A major concern of the participants at the Y2K Technical Workshop was that the main threat to facilities could be from external failures, such as electrical, natural gas, water and waste water utilities. The issue is much larger than any company,

municipality, or state. Only the federal government can adequately address the issue.

Many members of the chemical process industry are concerned about the reliability of power supply and are seeking ways to assess the vulnerability of their specific utility. Individual companies and local associations are encouraged to engage in dialogue with their individual power suppliers to find out what they are doing regarding Y2K. Accurate and pertinent information about utility status is essential for contingency planning purposes. However, for the purpose of this study, no effort was made to assess the potential of power outages from Y2K-related failures.

For some managers of facilities that draw high power loads prudent safety practice may determine that the plant be shut down during critical time periods and restarted at a later date. However, such decisions should not be made without communicating these planned actions with their utilities in order to prevent problems on the power grid. As a further complication, cumulatively, small power consumers can impact on power distribution through the nearly simultaneous shut down of many facilities without coordinating with their utility. Utilities can bring up or shutdown generators as demands vary, but they have trouble responding to unexpected changes in load or demand.

Insufficient electrical demand coupled with increased numbers of generators supplying the electric grid could overload the power distribution system, threaten the integrity of equipment, and/or trip breakers. If that happened, then there could be power outages for all the customers on the affected distribution line. The January 11, 1999 report, "Preparing the Electric Power Systems of North America for Transition to the Year 2000-A Status Report and Work Plan-Fourth Quarter 1998", issued a specific recommendation that would affect any advice given for facilities considering shutting down during rollover to Year 2000:[35]

> "Unusual Loading Patterns and Minimum Generation Conditions. Another priority concern that is emerging from the contingency planning process stems from the need to have additional generating units on line as a precaution against Y2K

events. With additional generators on line and the possibility of customer demand being low through the extended holiday period, utilities must consider what is called a *minimum generation* condition. When there is too much generation on line in relation to demand, system voltages and frequency can rise. Planning for the rollover into the Year 2000 must trade off the need to have additional reserves to respond to possible generator contingencies with the potential for excessive voltages. Customers should be encouraged during the period not to take unusual steps such as shutting down facilities that would normally operate through the holiday weekend. Extremely low demand or unusual pattern demand can present additional challenges for operation of the electric system."

The response to the utility problem has to be two-pronged, governmental leadership and corporate accountability. The federal government should ensure the integrity of the nation's electrical grid. In addition, state and local governments should make every effort to ensure the integrity of other utilities within their purview. The chemical process facilities should on the other hand design their Y2K compliance activities, particularly the contingency planning activities with the assumption that most utilities will fail, or at the best be under maximum strain.

Responsive Communication Among Stakeholders

Communication and trust between stakeholders is of tremendous importance in resolving Y2K related problems. Stakeholders, in the context of chemical safety, include: corporate and facility managers, operators, other workers, vendors, equipment manufacturers, unions, trade associations, regulators, non-regulatory agencies, emergency responders, insurance companies, community organizations and environmental organizations. Stakeholder communication has various aspects.

While logistic and timing problems may prevent a regulatory approach for assuring and communicating Y2K compliance to the public, the government should provide incentives to facilities to encourage them to voluntarily communicate to the public as clearly as possible the status of Y2K compliance. Given the extent of work being done for Y2K compliance, this communication will

avoid creating chaos and panic, allay public fears and promote rational behavior. Contingency planning, risk management, and decisions concerning shutdown must also involve communication amongst stakeholders.

Equally as important is the communication between different companies, both large and small, and communications across sectors of the economy. It is important to note that the complex interdependency of modern society assures that we are in this together. The sharing of information and building experience has a much greater chance of reducing or even completely eliminating the catastrophic threat of Y2K-related failures. Historically, safety-related issues are and should be treated on a non-competitive basis. For example, in the case of Y2K-related issues, the availability of a clearinghouse would constitute a major milestone in public reassurance.

Knowledge is key to responsive communication. Public agencies and the private sector already support training and education for chemical workers and Hazardous Materials (HAZMAT) emergency responders through programs which can tailor training modules to specific targeted groups of responders at the awareness, operations, technician and specialist levels. Y2K contingency planning and responsive communications are enhanced through training and education efforts developed to address the challenges of Y2K related incidents and scenarios.

For example, many organizations have active Emergency Response Teams. A program for cross-training of Y2K experts and emergency responders should assure that there is a comprehensive understanding of the incident command system on the one hand, with a detailed appreciation of how computerized systems control chemical process management.

Recommendations

Information Clearinghouse

The administration should promote the development of an information clearinghouse covering chemical process control systems, contingency planning, and other safety-related related Y2K issues.

An information clearinghouse should be developed to include chemical process control systems, contingency planning, and other related Y2K issues. The information could be tailored to specific industry sectors, i.e., propane distributors and users, chlorine facilities (water and wastewater units); and ammonia facilities. The clearinghouse could contain information specific to industry sectors such as:

- Checklists for inventories at different types of plants (large, medium-sized, and small; different chemicals and operations; batch process and continuous process);
- Listing of equipment and devices that have already been identified as having Y2K vulnerability and procedures to fix them;
- Testing procedures for different Y2K-vulnerable devices and equipment;
- Sources of further information and availability of resources for different types of organizations (particularly SMEs); and
- Items to consider in contingency planning.

A major obstacle in the development of a clearinghouse is the threat of litigation after-the-fact. A federal government agency should be the focal point for developing and maintaining the clearinghouse in coordination with other public and private entities. For this effort to be successful, the federal government must protect all organizations that are providing Y2K-related information for the public good, from the threat of lawsuits.

Contingency Planning and Readiness

The President's Council on the Year 2000 should coordinate the development of a contingency planning phase to build public awareness and promote the ability of emergency response infrastructure at the federal, state, and local levels to respond to environmental disruptions, chemical releases, and threats to worker and public health and safety. These activities should be coordinated with the activities initiated by the Federal Emergency Management Agency. In addition, the following specific recommendations should be considered for implementation:

- Batch processors should consider not beginning batches involving hazardous materials that will be in the process as the clocks turn to 2000 and at other sensitive dates, for processes where testing was not done or testing results were inconclusive.

- All processors that will run through the transition should have plans and sufficient and trained staff on hand to manually take control of the process. Facility managers should be prepared to shut down the process quickly and safely should control problems occur. Manual operations, especially over extended periods of time, may require significant changes in staffing and comprehensive training of managers, operators and other workers. The additional training, as appropriate, should be completed early in 1999.

- The EPA should promote the development of contingency plans to assure capable emergency response and promote communications among facilities, local governmental agencies and the nearby communities should problems arise.

- Facility managers should phase-in and coordinate shut downs, resulting either intentionally as a safeguard against Y2K-related failures or as a direct result of Y2K failures, and startups with local utilities and agencies, including emergency response agencies and Local Emergency Planning Committees.

- Chemical workers, emergency responders and local governmental agencies that focus on environmental health and emergency response should be provided with training and tools

(e.g., guidelines, checklists, and software) to address Y2K issues. Some initiatives have begun in this area.[36]

Utilities

As discussed earlier, power outages and other utility failures could constitute as much of a threat, or even more so, as internal process plant Y2K-related failures. Worker stress and chances for failure of controls will occur from emergency, accelerated shutdowns and subsequent startups. In addition, emergency response and other critical services could be impaired because of utility failures. Thus, utilities and oversight agencies should expend every effort to preserve the integrity of the national power grid system, local power supplies and other appropriate utilities. In addition, contingency plans should incorporate specific elements for communicating with utilities regarding each other's status.

Utilities, individually and through their associations, should take the lead in regards to 1. Informing their customers of possible power supply problems, and 2. Ascertaining whether their customers plan to alter their power demands such that utilities might be unable to maintain power distribution. Where utilities find significant planned shutdowns, they should take the initiative to coordinate shutdowns and subsequent start ups.

General

The following recommendations cover the whole range of issues ranging from incentives for Y2K compliance, SMEs, communication, and federal government role.

- Congress should create incentives Y2K compliance should be created using attractive tax write-offs for Y2K-related spending. This is probably the most effective method for enabling SMEs to actively pursue Y2K compliance programs. However, such programs should be developed with appropriate checks and balances to prevent unintended behaviors.

- Policy makers should develop small business loans for Y2K compliance with special emphasis on those businesses that are critical to public health and safety. The loans could be provided as low interest loans based on the production or handling of hazardous substances that generate the greatest potential for an impact to the workers and the public.

- Federal initiatives coordinated through the President's Council on the Year 2000 should include the organization of regional conferences focusing on ways to assess risks appropriately and how to prioritize which systems and facilities pose greater risks.

- EPA, OSHA and other safety organizations should increase Y2K awareness in SMEs by developing outreach campaigns, such as distributing Y2K awareness brochure to everyone on the Toxic Substances Control Act list, and other federal, state and local venues. Instrumentation and control vendors can and should be encouraged to increase their efforts in this communication activity.

- Communication tools should be developed to aid worker and public understanding. While it is critical to develop and implement Y2K compliance programs, it is equally important to inform workers and the public about the extensive work done so far in order to allay fears and avoid panic, and promote community contingency planning. In addition, efforts must be continued to communicate the seriousness of Y2K to SMEs and other organizations. This communication can be made through federal agencies, such as EPA, OSHA, and the Chemical Safety and Hazard Investigation Board (CSB), state and local agencies. Other important venues for outreach include: unions, trade and professional organizations, such as the American Institute of Chemical Engineers (AIChE), American Petroleum Institute (API), American Society of Safety Engineers (ASSE), Chemical Manufacturers Association (CMA), Chlorine Institute, and International Society for Measurement and Control (ISA), and research organizations such as the Mary Kay O'Connor Process Safety Center at Texas A&M University.

Endnotes:

[1] There is no specific regulatory mandate, which defines Y2K compliance. However, as used in this report, "Y2K Compliance" is intended to mean those recognized and generally accepted activities that must be implemented to maintain the operational integrity of a facility, prevent disruptions and accidents.

[2]See for example, http://gartner11.gartnerweb.com/public/static/aboutgg/pressrel/testimony1098.html

[3]The Year 2000 Information and Readiness Disclosure Act, Pub. L. No. 105- 271, signed by the President on October 19, 1998, primarily encourages good-faith disclosure of truthful Year 2000 information between businesses to avoid Year 2000 problems in information technology and other date-dependant embedded systems, especially in the critical segments of the economic infrastructure. The so-called "Good Samaritan" the Act raises the hurdle to those who would bring opportunistic lawsuits against technology providers, by making their evidentiary burden in any lawsuits higher. The Act responds to concern about bottlenecks to Year 2000 remediation due to failure of information sharing among businesses, their customers and suppliers, based on fear of legal liability. The Act recognizes the use of the Internet as a means of providing information about Year 2000 readiness, and also provides a limited, temporary exception to antitrust laws for Year 2000 information sharing among competitors within an industry. The Act does not provide any "immunity" to liability, and its evidentiary limitations specifically do NOT apply to Year 2000 statements made to end-user non-commercial consumers. See, http://www.itpolicy.gsa.gov/mks/yr2000/hill/s2392es.htm For an analysis of the Act see, http://www.itaa.org/govt/y2k/guidelines.htm

[4] John Koskinen, Chair of the President's Council on the Year 2000 Conversion, Opening remarks at the Y2K Expert Workshop held in Washington, DC on December 18, 1998.

[5] e-mail communication from Dan Daley, OxyChem

[6] See: http://es.epa.gov/oeca/eptdd/ocy2k.html.

[7] Letter from Mr. Emzell Blanton Jr., Deputy Assistant Secretary, OSHA.

[8] See http://www.oecd.org/ehs/y2k/index.htm

[9] See http://www.who.int/ifcs/y2k-intro.htm

[10] e-mail communication from Dr. Rebecca A. Head, Director, Washtenaw County Department of Environment and Infrastructure Services.

[11] e-mail from Mr. Joseph T. Hughes, Director, Worker Education and Training Program, National Institute of Environmental Health Sciences.

[12] See, http://www.naco.org/pubs/releases/y2ks.cfm.

[13] See, http://www.emergency.com/county2k.htm

[14] Frautschi, M.A., "Embedded Systems and the Year 2000 Problem (The Other Year 2000 Problem)," http://www.tmn.com/~frautsch/y2k2.html

[15] See, for example, the Y2K website of the National Institute for Occupational Safety and Health at: http://www.cdc.gov/niosh/y2k/y2k-hmpg.html

[16] *Large Property Damage Losses in the Hydrocarbon-Chemical Industries*. Marsh & McLennan, 14th edition, New York, NY, 1992.

[17] See, for example, *Guidance on year 2000 issues as they affect safety-related control systems* prepared by the United Kingdom's Health and Safety Executive: http://www.open.gov.uk/hse/year2000.pdf.

[18] Facilities usually divide systems into three categories: process control systems and components, business systems software and hardware, and infrastructure (or an "all other" category) which could include communication systems, security systems, loading racks, elevators, etc.

[19] For the Securities and Exchange Commission Interpretation of Disclosure of Year 2000 Issues and Consequences by Public Companies, Investment Advisers, Investment Companies, and Municipal Securities Issuers. See http://www.sec.gov/rules/concept/33-7558.htm

[20] Occidental's chemical operation, OxyChem, is a leading manufacturer of basic and chlorovinyl chemicals and specialty products. The company had sales of $4.3 billion in 1997, and presently operates 34 manufacturing facilities worldwide with more than 6,000 employees. OxyChem is the country's largest merchant marketer of chlorine and caustic soda, the number one producer of chrome chemicals and the second largest producer of sodium silicates. Worldwide, OxyChem is the top producer of potassium hydroxide and chlorinated isocyanurate products, the largest merchant marketer of ethylene dichloride (EDC) and a leading producer of phenolic molding compounds. See: http://www.oxychem.com

[21] Rohm and Haas began in 1909 as a partnership between innovative chemistry and business. Its origins trace back to pioneering work in leather tanning by Dr. Otto Rohm and Mr. Otto Haas. Today, Rohm and Haas is a manufacturer of specialty chemicals. Its products are those "invisible" ingredients that make things work better and last longer. The company's expertise in acrylic polymer design, electronic materials and chemical specialties make it one of the world's premier suppliers of specialty chemicals. Its products are made at 45 manufacturing plants located around the world. Sales take place in more than 100 countries and total more than $4 billion annually. The company's headquarters can be found on Independence Mall in Philadelphia, Pennsylvania. Rohm and Haas is a Delaware corporation whose stock is traded on the New York Stock Exchange under the symbol ROH. See: http://www.rohmhaas.com

[22] The audio and PowerPoint presentations are available at the Chemical Safety Board's website: http://www.chemsafety.gov.

[23] See for example, J.R. Stockton's critical dates at http://www.merlyn.demon.co.uk/critdate.htm.

[24] See, with access through Adobe Acrobat Reader, http://www.gao.gov/special.pubs/bcpguide.pdf

[25] It is very difficult to get SMEs to participate in meetings or workshops like the Y2K Technical Workshop sponsored by the Chemical Safety and Hazard Investigation Board. SMEs, in addition to lacking resources to participate in such activities, feel that their problems are much different than those experienced in larger companies and as such they can not gain anything useful by attending these meetings. This underscores the magnitude of the problem vis-à-vis SMEs, communication of Y2K information to SMEs, and ensuring SMEs to actively pursue programs and activities for Y2K readiness.

[26] "Measures relating to the Y2K problem in establishments where hazardous materials are handled: a study among establishments to which the AVR or EVR regulations apply," Drs. J. Massaar, Arbeidsinspectie (Health and Safety Inspectorate) The Netherlands, September 1998.

[27] See Appendix VII for a copy of Rockwell Automation's graphic depiction "Petroleum and Chemical Process" which provide a useful schematic insight into the scope of software and instrumentation involved in process controls. This is also accessible at: http://www.automation.rockwell.com/ind_ol/petro/PCMCProc.pdf

[28] http://www.honeywell.com/year2000/disclosure.stm

[29] http://www.honeywell.com/year2000/iac/producttesting.stm

[30] http://www.ragts.com/webstuff/y2k.nsf/Pages/Brands-Allen-Bradley?OpenDocument

[31] http://www.ragts.com/webstuff/y2k.nsf/2e3c24d93ace91788625659b005ff386/6c2235fc065f0147862566de005804e3/$FILE/Product+Test+Template.xls

[32] http://www.frco.com/fr/support/year2000/overview.doc

[33] phone discussion with Bruce Johnson, Y2K Compliance, Fisher-Rosemount

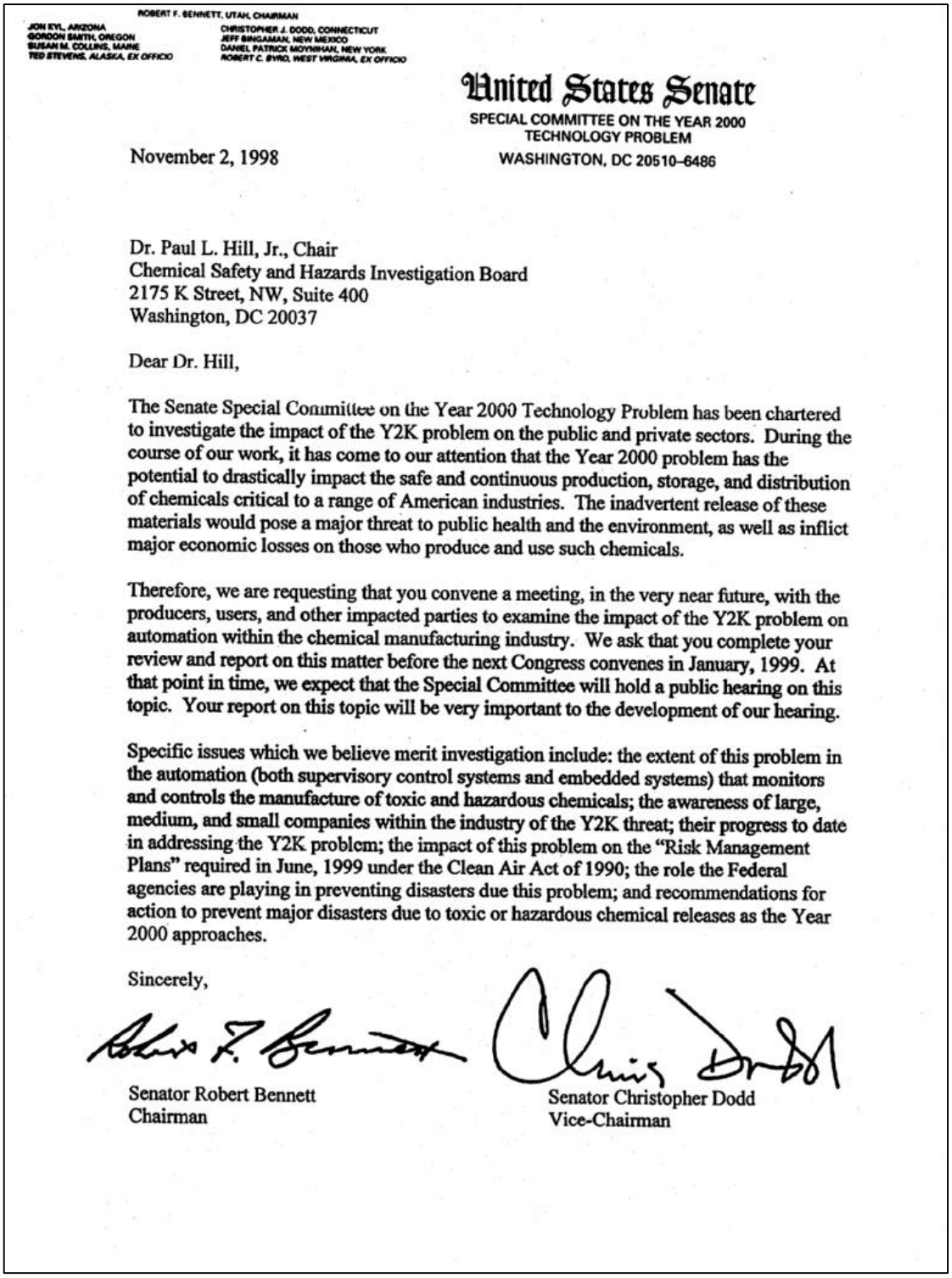
[34] http://www.frco.com/systems/products/y2k/index.dgw

[35] See with access though Adobe Acrobat Reader, ftp://ftp.nerc.com/pub/sys/all_updl/docs/y2k/secondfinalreporttodoe.pdf

[36] The National Institute of Environmental Health Sciences (NIEHS) Worker Education and Training Program will explore the inclusion of Year 2000 Conversion and Chemical Safety awareness and response in planned training activities for 1999. NIEHS in partnership with the EPA Superfund Hazardous Waste and Emergency Response Program and the DOE Nuclear Weapons Environmental Management Program will consider the development of appropriate curricula, training modules, training exercises and opportunities for providing technical information exchange in the development of an infrastructure for Y2K chemical emergency response. The Chemical Safety Board's Board Members will work with NIEHS as it coordinates activities in training hazardous chemical workers and chemical emergency responders.

Appendix I

Letter from the U.S. Senate Special Committee on the Year 2000 Technology Problem to the U.S. Chemical Safety and Hazard Investigation Board's Scientific Advisory Board



ROBERT F. BENNETT, UTAH, CHAIRMAN
JON KYL, ARIZONA
GORDON SMITH, OREGON
SUSAN M. COLLINS, MAINE
TED STEVENS, ALASKA, EX OFFICIO
CHRISTOPHER J. DODD, CONNECTICUT
JEFF BINGAMAN, NEW MEXICO
DANIEL PATRICK MOYNIHAN, NEW YORK
ROBERT C. BYRD, WEST VIRGINIA, EX OFFICIO

United States Senate
SPECIAL COMMITTEE ON THE YEAR 2000
TECHNOLOGY PROBLEM
WASHINGTON, DC 20510–6486

November 2, 1998

Dr. Paul L. Hill, Jr., Chair
Chemical Safety and Hazards Investigation Board
2175 K Street, NW, Suite 400
Washington, DC 20037

Dear Dr. Hill,

The Senate Special Committee on the Year 2000 Technology Problem has been chartered to investigate the impact of the Y2K problem on the public and private sectors. During the course of our work, it has come to our attention that the Year 2000 problem has the potential to drastically impact the safe and continuous production, storage, and distribution of chemicals critical to a range of American industries. The inadvertent release of these materials would pose a major threat to public health and the environment, as well as inflict major economic losses on those who produce and use such chemicals.

Therefore, we are requesting that you convene a meeting, in the very near future, with the producers, users, and other impacted parties to examine the impact of the Y2K problem on automation within the chemical manufacturing industry. We ask that you complete your review and report on this matter before the next Congress convenes in January, 1999. At that point in time, we expect that the Special Committee will hold a public hearing on this topic. Your report on this topic will be very important to the development of our hearing.

Specific issues which we believe merit investigation include: the extent of this problem in the automation (both supervisory control systems and embedded systems) that monitors and controls the manufacture of toxic and hazardous chemicals; the awareness of large, medium, and small companies within the industry of the Y2K threat; their progress to date in addressing the Y2K problem; the impact of this problem on the "Risk Management Plans" required in June, 1999 under the Clean Air Act of 1990; the role the Federal agencies are playing in preventing disasters due this problem; and recommendations for action to prevent major disasters due to toxic or hazardous chemical releases as the Year 2000 approaches.

Sincerely,

Senator Robert Bennett
Chairman

Senator Christopher Dodd
Vice-Chairman

Appendix II

Y2K Workshop Agenda and List of Participants

Agenda for Workshop on
The Year 2000 Technology Problem and Chemical Safety

Chemical Safety and Hazard Investigation Board
December 18, 1998
Hall of States, Washington, DC

8:15 – 8:30 AM	**Registration**
8:30 - 8:45	**Greetings: Chemical Safety Board, John Koskinen, President's Council on Y2K**
8:45 - 9:15	**Introductions**
9:15 – 9:35	**Presentation by OxyChem Corporation**
9:35 – 9:50	**Questions and Comments**
9:50 – 10:10	**Presentation by Rohm&Haas Company**
10:10 – 10:25	**Questions and Comments**
10:25 – 10:40	**Break**
10:40 – 11:40	**Identification of Critical Y2K Issues related to Chemical Accident Prevention**
11:40 – 12:30	**Priority Ranking of Issues**
12:30 – 1:30	**Lunch**
1:30 – 3:30	**Analysis of Priority Issues and Identification of Safety Gaps**
3:30 – 4-15	**Recommendations**
4:15 – 4:30	**Final Comments and Next Steps**
4:30	**Closing**

The Year 2000 Technology Problem and Chemical Safety Workshop Participants

Anderson, Joe
Oil, Chemical and Atomic Workers Union
255 Union Boulevard
Lakewood, CO 80228
Bus: (303) 987-5337
Bus Fax: (303) 987-5377
E-mail: JAnderson@ocaw.org

Bradshaw, Jerry
Texas A& M University
1012 Muirfield Village
College Station, TX 77845
Bus: (409)-845-0610
Bus Fax: (409) 845-6446
E-mail:j-bradshaw@tamu.edu

Brant, Robert
U.S. Chemical Safety Board
2175 K Street, NW #400
Washington, DC 20037
Bus: (202) 261-7619
Bus Fax: (202) 261-7650
E-mail: Bob.Brant@csb.gov

Brock, Kennith
HSB Industrial Risk Insurers
85 Woodland Street
Hartford, CT 06102
Bus: (860) 520-7332
Bus Fax: (860) 520-7559
E-mail: kenneth.brock@iri.com

Calhoun, Dennis
Citgo Petroleum
P.O. Box 3758
One Warren Place – 4 OWP
Tulsa, OK 74102
Bus: (918) 495-5724
Bus Fax: (918) 495-5339
E-mail: dcalhou@citgo.com

Corn, Jordan
Rohm and Haas Engineering Division
P.O. Box 584
Rte. 413 and State Rd.
Bristol, PA 19007
Bus: (215) 785-7029
Bus Fax: (215) 785-7080
E-mail: nasjc@rohmhaas.com

Daley, Daniel
Occidental Chemical Corporation
5005 LBJ Freeway
Dallas, TX 75244
Bus: (972) 404-2854
Bus Fax: (972) 404-3313
E-mail: dan.daley@oxy.com

Davis, George
ISA
67 Alexander Drive
Research Triangle Park, NC 27709
Bus: (919) 990-9244
Bus Fax: (919) 549-8211
E-mail: gdavis@isa.org

Dean, Norman
Center for Y2k and Society
1800 K Street, NW., Suite 400
Washington, DC 20006
Bus: (202) 775-3157
Bus Fax: (202) 775-3199
E-mail:ndean@csis.org

Duffy, Richard
International Association of Firefighters
1750 New York Avenue, NW.
Washington, DC 20006
Bus: (202) 737-8484
Bus Fax: (202) 737-8418
E-mail: iaffrmd@iaff.org

Epstein, Lois
Environmental Defense Fund
1875 Connecticut Avenue, NW., Suite 1016
Washington, DC 20009
Bus: (202) 387-3500
Bus Fax: (202) 234-6049
E-mail: lois_epstein@edf.org

Kathy Franklin
U.S. EPA, CEPPO
401 M Street, S.W.
Washington, DC 20460
Bus: (202) 260-8600
Bus Fax: (202) 260-7906
E-mail: franklin.kathy@epamail.epa.gov

Frautschi, Mark
Shakespeare and Tao Consulting
49 Merrion Court
Lutherville, MD 21093
Bus: (410) 453-9256
Bus Fax:
E-mail: frautsch@tmn.com

Frodyma, Frank
OSHA
U.S. Department of Labor
200 Constitution Avenue, NW., #S2315
Washington, DC 20210
Bus: (202) 693-2400
Bus Fax: (202) 693-2106
E-mail:

Goddard, Keith
Maryland Occupational Safety and Health
1100 North Eutaw Street
Room 613
Baltimore, MD 21201
Bus: (410) 767-2196
Bus Fax: (410) 767-2003
E-mail:keith.goddard@md_e_baltimore.osha.gov

Hart, Dave
Rockwell Automation
24701 Euclid Ave.
Cleveland, OH 44117-1794
Bus: (216) 266-7271
Bus Fax: (216) 266-7375
E-mail: dthart@ra.rockwell.com

Hayes, Ronald W.
SUNOCO
Ten Penn Center
1801 Market Street
Philadelphia, PA 19103
Bus: (215) 977-6189
Bus Fax: (215) 246-8797
E-mail: Ronald_W_Hayes@sunoil.com

Holler, Jim
ATSDR, Division of Toxicology
1600 Clifton Road, NE
Mailstop E-29
Atlanta, GA 30333
Bus: (404) 639-6309
Bus Fax: (404) 639-6315
E-mail: jsh2@cdc.gov

Hughes, Joseph
NIEHS
P.O. Box 12233
Research Triangle Park, NC 27709
Bus: (919) 541-0217
Bus Fax: (919) 541-0462
E-mail:hughes3@niehs.nih.gov

Hunter, Paul
U.S. Senate Special Committee
B-40, Suite 3
Washington, DC 20510-6486
Bus: (202) 224-5224
Bus Fax: (202) 228-0517
E-mail: paul_hunter@y2k.senate.gov

Isdale, Charles
Texas A&M University
511 E. University Drive, #208
P.O. Box 10297
College Station, TX 77843-3122
Bus: (409) 229-0320
Bus Fax: (409) 260-1371
E-mail: charles@isdale.com

Jones, Irene
Huntsman Corporation
3040 Post Oak Boulevard
Houston, TX 77056
Bus: (713) 235-6476
Bus Fax: (713) 235-6440
E-mail: irene_jones@huntsman.com

Kurland, David C
Rohm& Haas Company
100 Independence Mall West
Phildelphia, PA 19106-2399
Bus: (215) 592-3691
Bus Fax: (215) 592-3227
E-mail:david_c_kurland@rohmhaas.com

Lamar, Erik
International Association of Firefighters
1750 New York Avenue, NW
Washington, DC 20006
Bus: (202) 737-8484
Bus Fax: (202) 737-8418
E-mail:

Lawrence, Tom
RRS Engineering
459 Pine Hollow Court
St. Louis, MO 63021-6286
Bus: (314) 230-5302
E-mail:twlawr@swbell.net

Makris, Jim
U.S. EPA, CEPPO
401 M Street, S.W.
Washington, DC 20460
Bus: (202) 260-8600
Bus Fax: (202) 260-7906
E-mail:makris.jim@epa.gov

Mannan, Sam
Mary Kay O'Connor Safety Center
Texas A & M University
College Station, TX 77843-3122
Bus: (409) 862-3985
Bus Fax: (409) 862-3985
E-mail: mannan@tamu.edu

Matthiessen, Craig
U.S. EPA, CEPPO
401 M Street, S.W.
Washington, DC 20460
Bus: (202) 260-8600
Bus Fax: (202) 260-7906
E-mail:

McCully, Ruth
OSHA
U.S. Department of Labor
200 Constitution Avenue NW., #S2315
Washington, DC 20210
Bus: (202 693-2000
Bus Fax: (202) 693-2106
E-mail:

Millar, Fred
Consultant
5049 S. 7th Road, #201
Arlington, VA 22204
Bus: (703) 998-0996
E-mail: fmillar@erols.com

Morales, Oscar
U.S. EPA, OPPTS
401 M Street, S.W.
Washington, DC 20460

Newell, Bob
Honeywell, Inc.
16404 North Black Canyon Highway
Phoenix, AZ 85023-3033
Bus: (602) 313-5641
E-mail: bobnewell@iac.honeywell.com

Niemeier, Richard
NIOSH
4676 Columbia Parkway, M.S.C-14
Cincinnati, OH 45226
Bus: (513) 533-8388
Bus Fax: (513) 533-8588
E-mail: rwr1@cdc.gov.

O'Connor, Mike
Texas A&M University
2501 S. Mason Drive
Katy, TX 77450
Bus: (281) 578-9753
Bus Fax: (281) 578-9751
E-mail: mike_ocon@email.msn.com

Olson, Erik
Natural Resources Defense Council
1200 New York Avenue, NW, #400
Washington, DC 20005
Bus: (202) 289-2360
Bus Fax: (202) 289-0990
E-mail:eolson@nrdc.org

Paul Orum
Working Group on Community Right-to-Know
218 D Street, S.E.
Washington, DC 20003
Bus: (202) 544-9586
Bus Fax: (202) 546-2461
E-mail: orum@rtk.net Website: www.rtk.net/wcs

Poje, Jerry
U.S. Chemical Safety Board
2175 K Street, NW, #400
Washington, DC 20037
Bus: (202) 261-7617
Bus Fax: (202) 261-7650
E-mail:Poje@csb.gov

Rickett, Kate
U.S.EPA, OIRM
401 M Street, S.W.
Washington, DC 20460
Bus: (202)-260-2182
Bus Fax: (202)-260-6591
E-mail: rickett.katherine@epa.gov

Rosenthal, Isadore (Irv)
U.S. Chemical Safety Board
2175 K Street, NW, #400
Washington, DC 20037
Bus: (202) 261-7680
Bus Fax: (202) 261-7650
E-mail: Rosenthal@csb.gov

Scannell, Jerry
National Safety Council
1121 Spring Lake Drive
Itasca, IL 60143
Bus: (630) 775-2231
Bus Fax: (630) 285-9113
E-mail: Scannelj@nsc.org

Sepeda, Adrian
Occidental Chemical Corporation
5005 LBJ Freeway
Dallas, TX 75244
Bus: (972) 404-3273
Bus Fax: (972) 404-3219
E-mail: adrian_l_sepeda@oxy.com

Skinner, Ray
U.S. Department of Labor
Area Director Houston South OSHA Area Office
17625 El Camino Real Suite 400
Houston, TX 77058
(281) 286-0583
(281) 286-6352
E-mail:

Smerko, Robert
The Chlorine Institute
2001 L Street, NW, #506
Washington, DC 20036-4919
Bus: (202) 872-4729
Bus Fax: (202) 223-7225
E-mail:rsmerko@cl2.com

Speights, David
U.S. EPA, CEPPO
401 M Street, S.W., Rm 5104
Washington, DC 20460
Bus: (202) 260-8600
Bus Fax: (202) 260-7906
E-mail: speights.david@epa.gov

Sprinker, Michael L.
International Chemical Workers
Union Council/UFCW
1655 West Market Street
Akron, OH 44313
Bus: (330) 867-2444
Bus Fax: (330) 867-0544
E-mail: 104525.706@compuserve.com

Stavrianidis, Paris
Factory Mutual
1151 Boston Providence Pike
P.O. Box 9102
Norwood, MA 02062
Bus: (781) 255-4983
Bus Fax: (781) 255-4024
Paris.stavrianidis@factory.mutual.com

Summers, Angela
Premier Consulting - Engineering
Triconex Corporation
4916 FM 1765
LaMarque, TX 77568
Bus: (409) 933-1199
Bus Fax: (409) 935-3555
E-mail:asummers@systems.triconex.com

Susil, John
Celanese Ltd.
P.O. Box 819005
Dallas, TX 75381-9005
Bus: (972) 443-3757
Bus Fax: (972) 277-8595
E-mail:jcsusil@celanese.com

Taylor, Andrea Kidd
U.S. Chemical Safety Board
2175 K Street, NW, #400
Washington, DC 20037
Bus: (202) 261-7600
Bus Fax: (202) 261-7650
E-mail: Taylor@csb.gov

Viederman, Stephen
Jessie Smith Noyes Foundation
6 East 39th Street
New York, NY 10016
Bus: (212) 684-6577
Bus Fax: (212) 689-6549
E-mail: stevev@noyes.org

Weaver, Jack
American Institute of Chemical Engineers
3 Park Avenue
New York, NY 10016-5901
Bus: (212) 591-7407
Bus Fax: (212) 591-8895
E-mail: jackw@aiche.org

West, Harry
Shawnee Engineers, Inc.
1415 North Loop West, #1150
Houston, TX 77008
Bus: (713) 861-3889
Bus Fax: (713) 868-9948
E-mail:hhwest@pdq.net

Appendix III

Example Checklist of Devices to be Checked for Year 2000 Compliance for a Hypothetical Chemical Plant

Example Checklist of Devices to be Checked for Year 2000 Compliance for a Hypothetical Chemical Plant

COMPONENT (to check for compliance)	Worst Case Failure Effects
Embedded Microchips	
Controllers	
Weighers	In accurate readings resulting in poor conversion
Reactor	
Charging	Wrong amounts reacting-poor conversion
Temperature	Poor conversion-explosion
Pressure	Poor conversion-explosion
Cleaning	Inaccurate timing-process interruption-release
Stripper	Contamination of product
Dryer	Water contamination of product
Centrifuge	Poor separation
Storage	Overflow-release
Video Cameras	Failure to work
Still Cameras	Failure to work
Alarm Systems	Failure to work
Clocks	Show incorrect time
Elevators	Failure to work
Phones	Failure to work
Answering Machines	Failure to work
Software	
Main frame, network, desktop, & communication computers	Data generated errors may result in inaccurate data or system failures
Office computers	
Purchasing	No supplies
Inventory	Excess supplies
Distribution	Will send out incorrect orders
Sales	Will not be able to keep up with orders
Accounting	Will compute incorrectly
Personnel	Will not be kept up correctly
Process Computers	
Control	Explosion-release
Transportation	Buildup of stock
Quality Control	Poor quality

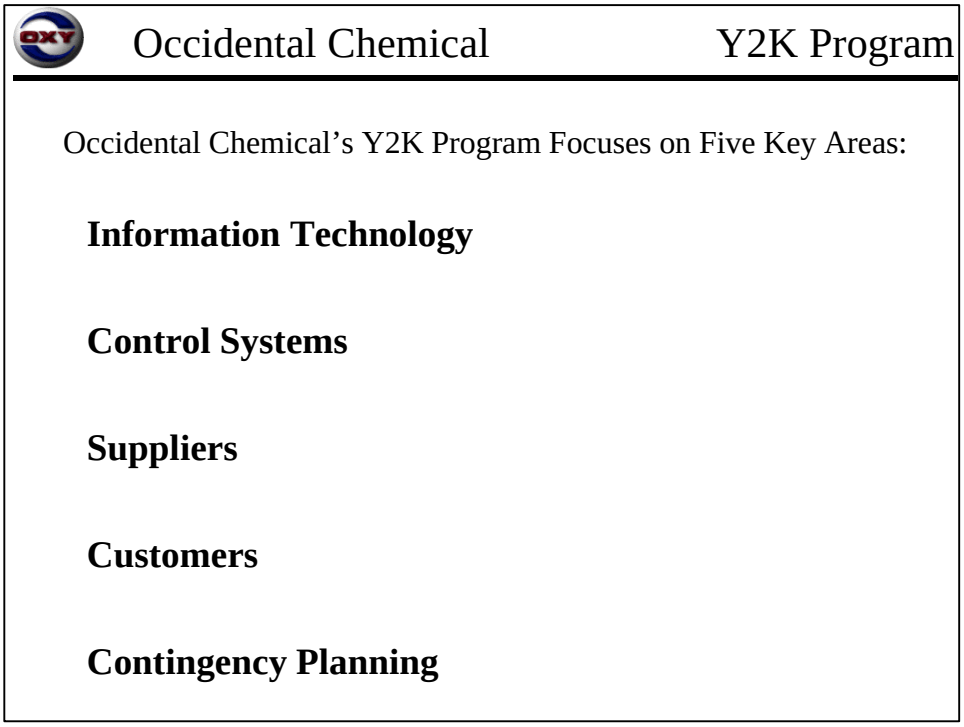
EXAMPLE CHECKLIST OF DEVICES TO BE CHECKED FOR YEAR 2000 COMPLIANCE FOR AN HYPOTHETICAL CHEMICAL PLANT
(Continued)

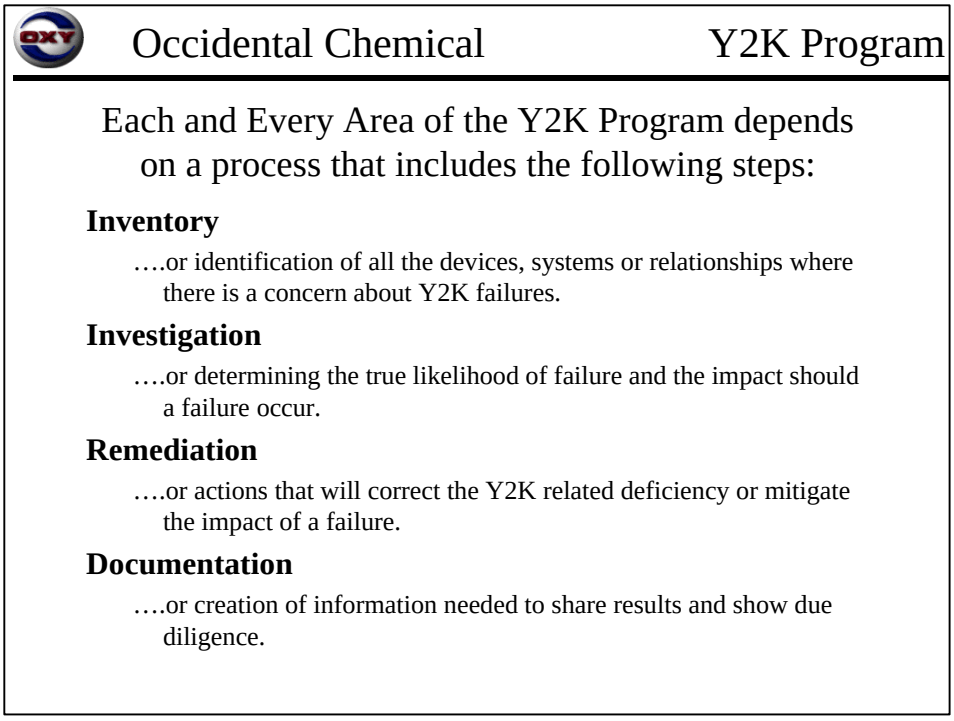
COMPONENT (to check for compliance)	**Worst Case Failure Effects**
Supply Chain	
Utilities	
Electricity	Process shut down
Water	Process shut down
Waste	Waste buildup beyond capabilities
Communications	No communication
Raw material suppliers	
Primary feedstock	Process shut down
Initiator-catalyst	Process shut down
Service providers	
Insurance	Extra expenses
Hospitals	No medical care
Vending	No food
Customers	No incoming funds
Security	
Video cameras	Failure to work
Security lights	Failure to work
Access	
Parking	Failure to work
Building	Failure to work
Room	Failure to work
Alarms	
Fire	Failure to work
Intrusion	Failure to work
Warning	Failure to work
Process	Failure to work

Note: The information given in this table is provided as an example only. Checklists like this should be developed on an individual plant-specific basis using criteria and knowledge that are unique to the plant.

Appendix IV

Occidental Chemical's Workshop Presentation on Year 2000 Compliance Efforts





Occidental Chemical Y2K Program

When focusing on Process Plant Safety, the two most important parts of the Y2K Program are:

IT

Control Systems

Suppliers

Customers

Contingency Planning

Control Systems

…or the process being used to identify and correct the problems associated with microprocessors and programming that is embedded in systems and devices used to monitor and control process plants.

Contingency Planning

…or the process being used to identify the likely scenario and make plans to deal with it AND to surface possible situations and to ensure ability to respond to them.

Occidental Chemical Y2K Program

Handling Control Systems includes the following elements:

Inventory

- Identify ALL systems and devices containing microprocessors and programming.
- Prioritize all identified items according to both "likelihood" of failure and "Impact" should a failure occur.

Investigate

- Create a standard methodology for investigating devices - Include:
  - Triage by priority - eliminate low/low items
  - Shared Information - eliminate items screened elsewhere
  - Vendor Information - eliminate items vendors have tested and confirmed to be compliant or not a Y2K device.
  - Physical Inspections - Battery or Digital vs. Analog signals
  - Details Testing - Rigorous preparation and execution
- Create Database to Record Results and Share Information
  - Think about end results before starting Database design
  - Don't spend all your time working on the "means to the end"
- Provide Adequate Technical Support. While not a particularly technically demanding issue, there are some important subtleties about Y2K.
  - Clock cycle issues
  - Integration and Inter-relationships
  - Overall process flow - Focusing in on the right things.
  - Y2K Issues that will not occur in the year 2000 or integrating Y2K thinking in everyday business.

Occidental Chemical Y2K Program

Handling Control Systems (continued):

Remediate

- Create a standard methodology to streamline getting things done.
  - Don't try to be opportunistic …. fix the Y2K problem
  - Take patches and fixes supplied by vendors
  - When a vendor doesn't have a plan …. fire up the steam roller
  - This is not the time for normal budget cycles
- Track remediation to ensure closure
- Test after remediation

Document

- Create a minimum standard requirement for documentation
  - Describe What, Who, When, Where
  - Don't duplicate
  - Audit while work is being done

Occidental Chemical Y2K Program

Addressing Contingency Planning includes the following elements:

Preparing for the "Most likely worst case scenario."

- What is the likely scenario for IT Systems?
- What is the likely scenario for Control Systems?
- What is the likely scenario for suppliers?
- What is the likely scenario for close-linked customers and other customers?
- What is the likely scenario for for the surrounding community?
- Create a "composite" scenario. Assume that multiple problems occur simultaneously.
  - Conduct "What-if" exercises
  - Conduct Table Top exercises

Preparing for Emergency Response.

- Identify "Unlikely" situations.
- Identify "Unrecognized" situations.
  - You know where your focused your attention.
    - What did you take for granted?
- Identify recognized situation you have been "Unable to address".
- Test Emergency Response capacity in addressing situation described above.

Occidental Chemical Y2K Program

Successful Y2K programs will incorporate the following characteristics:

Project Management

- Upon his arrival at the Death Star, where construction was behind, Darth Vader's entering line was "I'm here to put you back on schedule." You'll need a Darth Vader.

Process Development

- No one has ever addressed Y2K before …. and it doesn't come naturally. You'll need someone who understands and can articulate how the process will work in a plant.

Process Implementation

- There have been billions of dollar and million of man-hours spent on process re-design in the last ten years ---- go find one that is working as intended. You'll need someone who can get things functioning as designed across a wide variety of sites.

Accountability/Authority

- Y2K is one of those things most people would like to see just go away …. it won't go away. You'll need to point at someone and say "It's your job." That person will need the resources to do his or her job.
- Normal methods of resource allocation will hinder progress. You'll have to decide if you can stand the delays.

Occidental Chemical Y2K Program

Occidental Chemical's Y2K Contingency Program Has Three Main components:

Contingency Level 1:

Continued Safe Operations

Contingency Level 2:

Safe Shut Down

Contingency Level 3:

Emergency Response

Occidental Chemical Y2K Program

Contingency Level 1: Continued Safe Operations

Those things necessary to keep the facility operating in a safe and environmentally sound manner…

Should the Y2K Program Steps fail to prevent a problem, …

what pre planned actions can be taken that would allow the facility to continue operations safely and in an environmentally sound manner?

Occidental Chemical Y2K Program

Contingency Level 1: Continued Safe Operations Examples

- Minimize finished product inventories and waste/effluent levels to allow as much reaction time as possible to unusual situations
- Maximize raw material inventories (within safe limits) in case your supplier fails
- If you purchase a small amount of steam, you should consider renting a mobile steam generator for back up should your supplier fail
- "Ditto" for air or nitrogen with bottled gas for back up
- Consider low tech/cheap walki-talkies to back up sophisticated communication systems

Occidental Chemical Y2K Program

Contingency Level 1: Continued Safe Operations Examples (Cont.)

- Increase operations & craftsman staffing during critical periods to be able to quickly respond to unusual situations
- Shut down non essential units; restart them later after critical periods have passed and essential units are running well
- Make pre arrangements with trucking firms to handle material if primary transportation modes are not available
- Develop a plan to manually control output from variable frequency drive controllers (switch to fixed speed and control volume output via dampers, valves, etc.)
- Identify and test manual overrides for security systems

Occidental Chemical Y2K Program

Contingency Level 2: Safe Shut Down

Those things necessary to shut the facility down in a safe and environmentally sound manner…

Should the Y2K Program Steps fail to prevent a problem, and the Contingency Level 1 plans fail to keep the facility operating safely, ...

what pre planned actions can be taken that would allow a safe and environmentally sound shut down of the facility?

Occidental Chemical Y2K Program

Contingency Level 2: Safe Shut Down Examples

- Rent portable electrical generators or lights for emergency use
- Icrease operations & craftsmen staffing during critical periods to monitor and react quickly for shut down purposes
- Shut down non essential equipment before critical periods to allow more attention time for shut down of critical systems
- Ensure (test) all emergency shut down equipment and safety systems are fully functional before critical periods
- Test UPS back up systems to ensure power is supplied to control systems that allow safe shut down

Occidental Chemical Y2K Program

Contingency Level 2: Safe Shut Down Examples (Cont.)

- Consider having a back up low tech. communication system for use in plant if the main system fails
- Pre test emergency vent scrubbing systems to eliminate or minimize emissions during shut down
- Conduct S/D drills--consider more than one system failure

Occidental Chemical Y2K Program

Contingency Level 3: Emergency Response

Those things necessary for an adequate and proper emergency response to facility incidents…

Should the Y2K Program Steps fail to prevent a problem,
and the Contingency Level 1 plans fail to keep the facility operating safely,
and the Contingency Level 2 plans fail to shut the facility down safely, ...

what pre planned actions can be taken that would ensure adequate and proper emergency response to facility incidents?

Occidental Chemical Y2K Program

Contingency Level 3: Emergency Response Examples

- Consider having the Plant Emergency Response Team on "Active" stand-by
- Work with "outside" responders and pre plan a back up communication mechanism and practice a response plan
- Develop a system to warn neighbors in case the local emergency warning system fails
- Conduct drills considering multiple system failures
  - Internally
  - With "outside" response agencies

Appendix V

Rohm and Haas' Workshop Presentation on Year 2000 Compliance Efforts

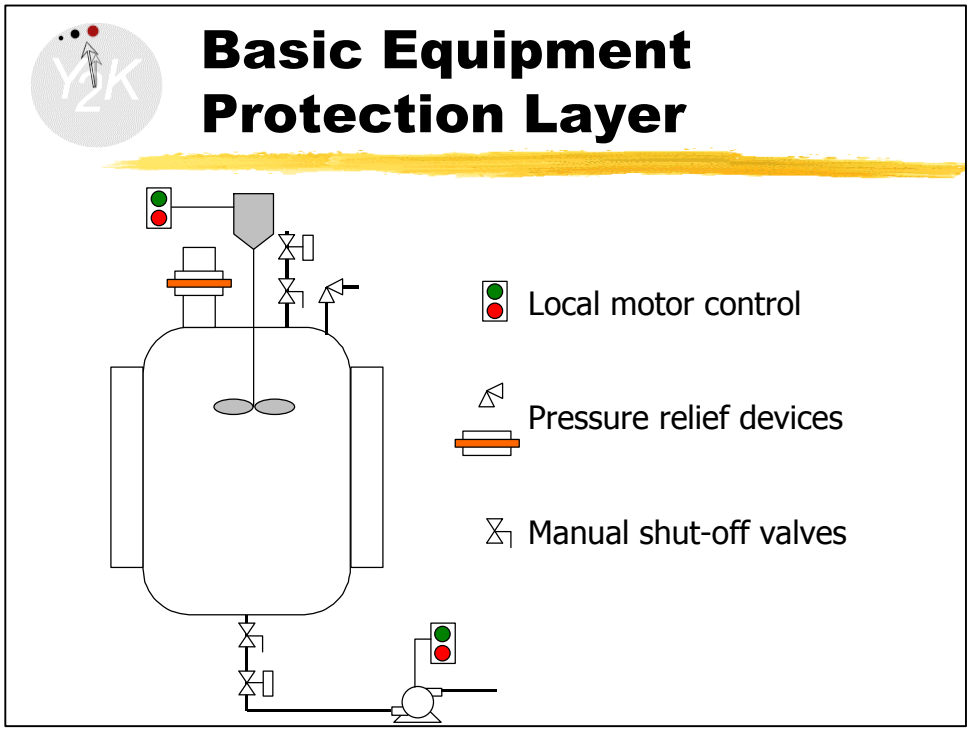
Chemical Process Safety and the Year 2000

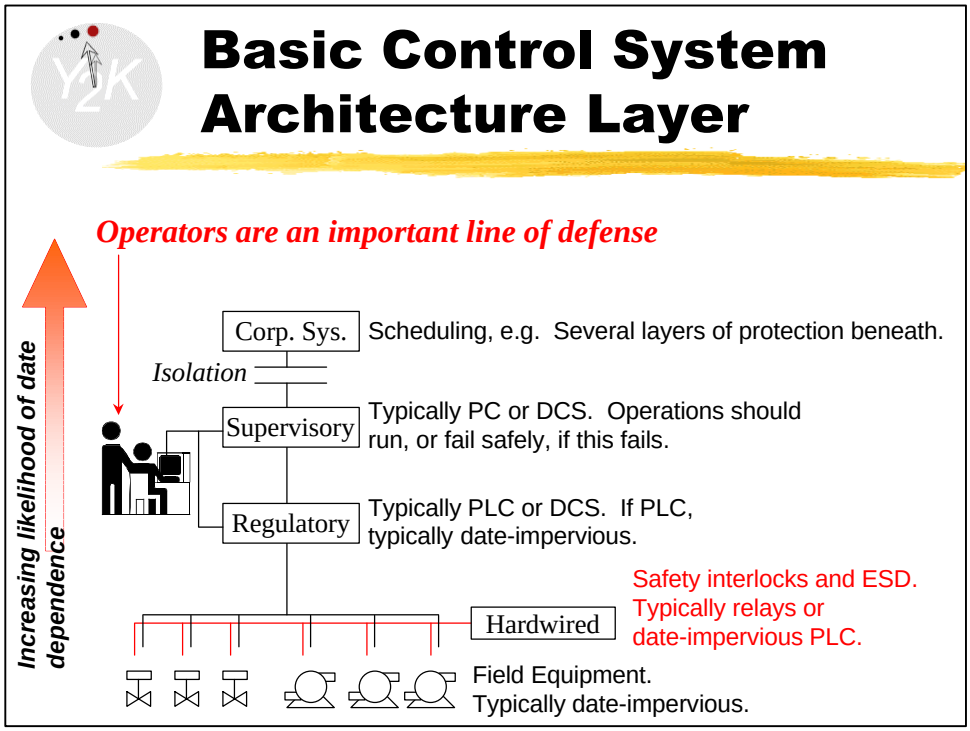
- Basic process control safety
- The implications of Y2K
- Program overview
  - Scope
  - Requirements
- Findings
- A final layer of protection

The Layers of Protection in a System

- Any physical device can - and **will**, at some point - fail
- Systems must be designed to withstand failures
- Failure protection is layered:
  - Basic equipment protection
  - Basic control system architecture
  - Fail-safe design
  - Operators and engineers
  - Administrative procedures

Increasing Robustness


Basic Equipment Protection Layer
Local motor control
Pressure relief devices
Manual shut-off valves


Basic Control System Architecture Layer
Operators are an important line of defense
Increasing likelihood of date dependence
Corp. Sys.
Scheduling, e.g. Several layers of protection beneath.
Isolation
Supervisory
Typically PC or DCS. Operations should run, or fail safely, if this fails.
Regulatory
Typically PLC or DCS. If PLC, typically date-impervious.
Safety interlocks and ESD. Typically relays or date-impervious PLC.
Hardwired
Field Equipment. Typically date-impervious.

Fail-Safe Design Layer

- Systems are designed to fail safely
- Facilities and control systems are designed to withstand the loss of:
  - Process and control devices
  - Power
  - Water
  - Other utilities
- All systems are subject to formal design reviews:
  - HAZOP
  - Failure modes and effects analysis
- System design emphasizes ability to achieve safe shutdown

The Implications of Year 2000

- Systems and processes are designed to deal with single failures
- Year 2000 could cause multiple concurrent failures
  - Control failures
  - Utilities
- Safe design and a Year 2000 program provide good protection against multiple control failures
- Greatest exposure is in utility failures

Rohm and Haas Corporate Policy

Rohm and Haas Company is committed to identifying and correcting date-based problems in computer systems (hardware and software), commonly referred to as the "Year 2000 Problem", so that all critical operations continue without disruption.

This policy applies to all Company units, world-wide, including subsidiaries, joint ventures, and other related units.

Rohm and Haas Scope

- Business computer systems
- Technical infrastructure
- End-user computing
- Customers and suppliers
- **Manufacturing and warehousing**
- **Environmental**
- Research and development
- Other

Two Classes of Manufacturing Systems

- Process control systems
- Other physical systems

- Similar approach for both
- Slightly different requirements for each class
- Both efforts coordinated by same group

Control Systems Scope

Computer-based equipment that directly controls the manufacture of chemicals, e.g.:

- Process control computers
  - Distributed control systems
  - Programmable logic controllers
  - PCs
- Purchased equipment containing computers

Pneumatic and electromechanical control is excluded

Other Physical Systems Scope

- *Physical plant equipment* used in the manufacturing process, e.g.:
  - Raw material handling systems
  - Equipment monitoring systems
  - Waste treatment systems
- *Physical equipment* necessary to ensure uninterrupted operation of the plant, e.g.:
  - Fire detection and suppression systems
  - Perimeter security systems
  - HVAC systems

Why the Distinction? How We Started

- Original focus was on control systems
  - Highest degree of risk
  - Strong central understanding
  - Central leverage with key suppliers
  - Consistent approach to critical systems needed
- Intended to let sites manage other physical equipment independently
  - Range of equipment significantly more diverse
  - Most selection and procurement was local

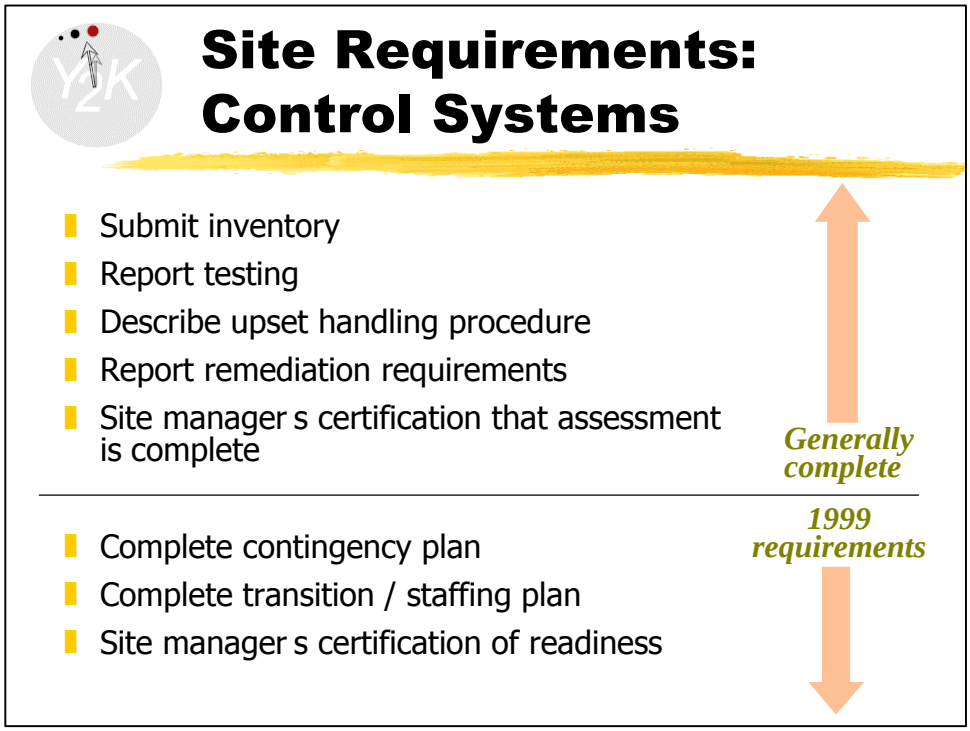
Physical Systems Added to Central Program

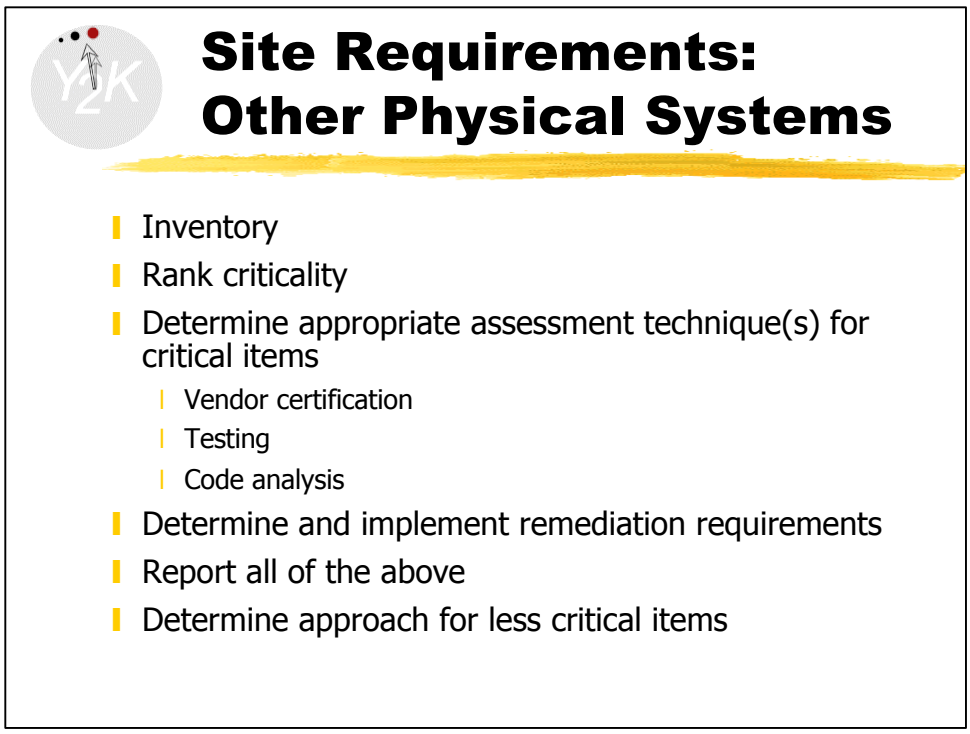
- Different sites took very different approaches to physical systems
- Some overlap between control and other physical systems became apparent
- Found that there would be benefit in central organization
  - Better communication and information sharing
  - More uniform guidelines
  - Corporate view of status and issues at each site

Site Requirements: Control Systems

- Each site is required to build a five-tier safety net:
  - Obtain vendor certification of **every** control component
  - Test **every** system - demonstrate ability to produce
  - Analyze code where critical

  - Arrange technical coverage through and beyond midnight
  - Be prepared to identify and handle upsets and to shut down safely if necessary


Site Requirements:
Control Systems
Submit inventory
Report testing
Describe upset handling procedure
Report remediation requirements
Site manager s certification that assessment is complete
Generally complete
1999 requirements
Complete contingency plan
Complete transition / staffing plan
Site manager s certification of readiness


Site Requirements:
Other Physical Systems
Inventory
Rank criticality
Determine appropriate assessment technique(s) for critical items
Vendor certification
Testing
Code analysis
Determine and implement remediation requirements
Report all of the above
Determine approach for less critical items

Findings: Control Systems

- **Every** failure found was predicted by the vendor
- Use of dates limited to data acquisition and reporting
- Old control systems require upgrades
- Vendors are generally cooperative
- To date, have found only one catastrophic control system failure

Findings: Other Physical Systems

- About 5-7% of physical systems require remediation
- Typically involve PC upgrades
- Have found no catastrophic failures of physical systems
- Many identified failures have straightforward workarounds
  - Manual reset of date after 1/1/00
  - Elimination of systems
  - Manual intervention
  - Do nothing - noncompliance is inconvenient, but acceptable

A Final Protection Layer

- Most major problems occur while a plant is running
- Shutting down operations through the millennium transition is a prudent precaution, where practical
- Many of our plants are traditionally idle at year-end, and will be for the transition
- Planned shutdown for other sites is under consideration as part of contingency planning

Appendix VI

Process Control and Instrumentation Vendor Web Site Addresses

Process Control and Instrumentation Vendor Web Site Addresses

ABB
http://www.abb.com/usa/Corporate/index.asp?ref=year2000.htm;ing=1

Allen-Bradley
http://www.ragts.com/webstuff/y2k.nsf/Pages/Brands-Allen-Bradley?OpenDocument

Elsag Bailey Process Automation
http://www.ebpa.com/y2k

Fisher-Rosemount
http://frco.com/fr/support/year2000/overview.doc

Foxboro
http://foxboro.com/y2000/index.htm

Honeywell
http://www.honeywell.com/year2000/

Moore Products
http://www.mooreproducts.com/Y2K/default.htm

Schneider Automation (Modicon, Square D, and Telemecanique)
http://www.modicon.com/

Siemens
http://www.ad.siemens.de/meta/html_76/year2000.shtml

Toshiba
http://www.tic.toshiba.com/html/y2k.htm

Triconex
http://www.triconex.com

Wonderware
http://www.wonderware.com/framecontrol.asp?Body=/News/NewsY2000.htm&Left=/corporateinfo/Left/wwleft.htm&Top=/corporateinfo/Top/wwtop.htm

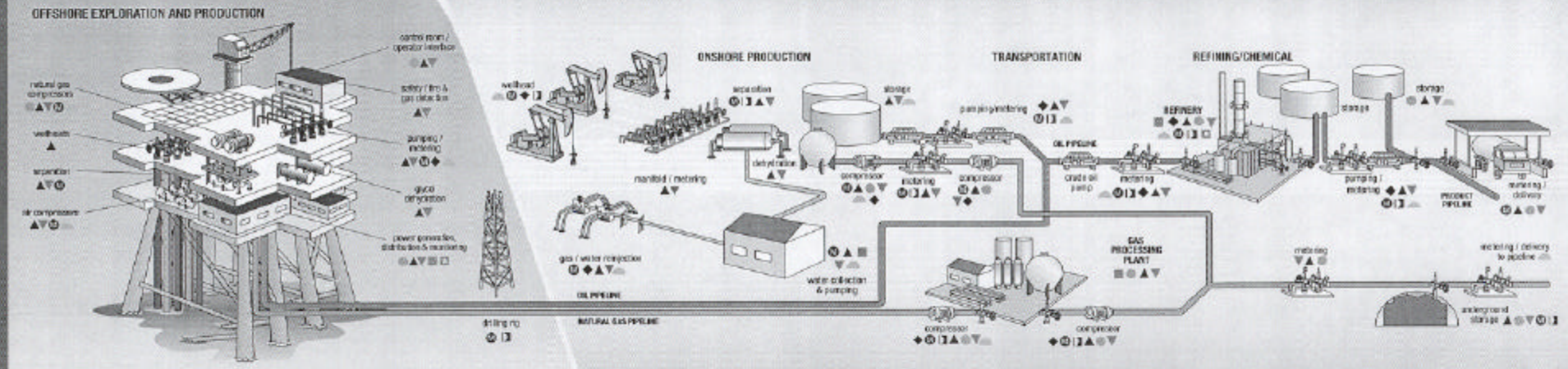
Yokogawa
http://www.yokogawa-ia.com/corporate/yr2000.htm

Appendix VII

Graphic Depiction of Petroleum and Chemical Processes

See Next Page

Petroleum & Chemical Process



- Operator Interface
- PLC®, SLC™, MicroLogix™ and ControlLogix™ Controllers
- Power Monitoring Software, RSView32™ Software
- Reliance Electric & Allen-Bradley Drives and Rockwell Automation Drive Systems
- Reliance Electric Motors
- Industrial Control (Push Buttons, Pilot Lights, Contactors, Starters, Terminal Blocks, Switches, Relays)
- DODGE Belts, Sheaves, Couplings, Gear Boxes, Mounted Bearings
- CENTERLINE® Motor Control Centers
- Medium Voltage Control (MV Vacuum Contactors, MV Soft Starters and MV AC Drives)

Rockwell Automation

Appendix VIII

Summary of Risk Management Programs Mandated by the Clean Air Act Amendment of 1990

United States Environmental Protection Agency | Office of Solid Waste and Emergency Response (5101) | 550-F-96-002 May 1996

EPA
CEPP

RISK MANAGEMENT PLANNING: ACCIDENTAL RELEASE PREVENTION

Final Rule: Clean Air Act section 112(r)

FACTSHEET

Preventing accidental releases of hazardous chemicals is the shared responsibility of industry, government, and the public. The first steps toward accident prevention are identifying the hazards and assessing the risks. Once information about chemicals is openly shared, industry, government, and the community can work together toward reducing the risk to public health and the environment. Important new provisions in the Clean Air Act advance the process of risk management planning and public disclosure of risk. These requirements will affect facilities that produce, handle, process, distribute, or store certain chemicals. The final rule for risk management planning was promulgated on 20 June 1996.

MANAGING CHEMICALS SAFELY

Section 112(r) of the amended Clean Air Act (CAA), signed into law on 15 November 1990, mandates a new federal focus on the prevention of chemical accidents. The objective of section 112(r) is to prevent serious chemical accidents that have the potential to affect public health and the environment. Under these requirements, industry has the obligation to prevent accidents, operate safely, and manage hazardous chemicals in a safe and responsible way. Government, the public, and many other groups also have a stake in chemical safety and must be partners with industry for accident prevention to be successful.

The risk management planning requirements of CAA section 112(r) complement and support the Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA). A milestone in federal actions, EPCRA helps local communities prepare for and respond to chemical accidents. It requires communities to develop emergency response plans, based on information from industry concerning hazardous chemicals. Under the new CAA requirements, stationary sources (facilities) must identify and assess their chemical hazards and carry out certain activities designed to reduce the likelihood and severity of accidental chemical releases. Information summarizing these activities will be available to state and local governments, the public, and all other stakeholders. Using this information, citizens will have the opportunity to work with industry to reduce risks to the community from chemical accidents.

In the broadest sense, risk management planning relates to local emergency preparedness and response, to pollution prevention at facilities, and to worker safety. In a more focussed sense, it forms one element of an integrated approach to safety and complements existing industry codes and standards. The risk management planning requirements build on OSHA's Process Safety Management Standard, the chemical safety guidelines of the Center for Chemical Process Safety of the American Institute of Chemical Engineers, and

similar standards of the American Petroleum Institute and Chemical Manufacturers Association, as well as the practices of many other safety-conscious companies.

IT'S THE LAW...

CAA section 112(r) mandates that EPA publish rules and guidance for chemical accident prevention. These rules must include requirements for sources to develop and implement risk management programs that incorporate three elements: a hazard assessment, a prevention program, and an emergency response program. These programs are to be summarized in a risk management plan (RMP) that will be made available to state and local government agencies and the public.

WHO'S COVERED

Any source with more than a threshold quantity of a listed "regulated substance" in a single process must comply with the regulation. "Process," in terms of the regulation, means manufacturing, storing, distributing, handling, or using a regulated substance in any other way. Transportation, including pipelines and vehicles under active shipping orders, is excluded. On 31 January 1994, EPA promulgated a final list of 139 regulated substances: 77 acutely toxic substances, 63 flammable gases and volatile liquids, and Division 1.1 high explosives as listed by DOT. The final list rule established threshold quantities for toxics ranging from 500 to 20,000 pounds. For all listed flammables, the threshold quantity is 10,000 pounds. EPA proposed modifications to the final list on 15 April 1996. These modifications would exclude facilities handling explosives, exploration/production facilities for oil and gas, and gasoline.

EPA estimates that approximately 66,000 sources will be covered by the rule, assuming the proposed list amendments are adopted. The universe includes chemical manufacturers, other manufacturers, certain wholesalers and retailers, drinking water systems, wastewater treatment works, ammonia refrigeration systems, utilities, and federal facilities. Sources with at least one covered process must comply with the rule by June 20, 1999.

THREE LEVELS OF COMPLIANCE

The final risk management planning regulation (40 CFR part 68) defines the activities sources must undertake to address the risks posed by regulated substances in covered processes. To ensure that individual processes are subject to appropriate requirements that match their size and the risks they may pose, EPA has classified them into three categories ("Programs").

Program 1 requirements apply to processes for which a worst-case release, as evaluated in the hazard assessment, would not affect the public. These are sources or processes that have not had an accidental release that caused serious offsite consequences. Remotely located sources and processes using listed flammables are primarily those eligible for this program.

Program 2 requirements apply to less complex operations that do not involve chemical processing (e.g., retailers, propane users, non-chemical manufacturers, and other processes not regulated under OSHA's PSM Standard).

Program 3 requirements apply to higher risk, complex chemical processing operations and to processes already subject to the OSHA PSM.

RMP BASICS

Sources with processes with a regulated substance above a threshold quantity will be required to carry out the following elements of risk management planning:

◆ ***An offsite consequence analysis that evaluates specific potential release scenarios, including worst-case and alternative***

scenarios

- ***A 5-year history of certain accidental releases of regulated substances from covered processes***
- ***An integrated prevention program to manage risk***
- ***An emergency response program***
- ***An overall management system to supervise the implementation of these program elements***
- ***A risk management plan (RMP), revised at least once every five years, that summarizes and documents these activities for all covered processes***

Based on their limited potential for serious offsite consequences, sources are not required to implement a prevention program, an emergency response program, or a management system for Program 1 processes. Sources with processes in Program 2 and Program 3 must address each of the above elements.

LINKS

The OSHA PSM Standard (29 CFR 1910.119) reflects the key elements that the petrochemical industry, trade associations, and engineering societies have deemed essential to safe management of hazardous substances for complex, chemical-processing operations. EPA has adopted OSHA's PSM requirements as the Program 3 prevention program, with only minor changes in terminology. With few exceptions, processes assigned to Program 3 are already subject to the OSHA PSM Standard; the remaining Program 3 processes are in industry sectors that have a significant accident history.

EPA has also worked closely with other regulatory programs that focus on risk management issues for hazardous chemicals in order to foster co-ordination and reduce burden. EPA and the National Response Team have prepared Integrated Contingency Plan Guidance to assist sources subject to multiple regulations in preparing a consolidated emergency response plan. Further, EPA believes that many of the prevention program requirements for Program 2 processes and the emergency response program requirements can be satisfied without additional effort because of existing compliance with other federal and state regulations, industry standards and codes, and good engineering practices.

MAKING IT WORK

To document compliance with the rule and provide risk information, all sources must submit to a central location a risk management plan that includes a registration, an executive summary, a 5-year accident history, and offsite consequence analysis information. Sources with Program 2 and 3 processes also must submit information in the RMP regarding compliance with requirements for the prevention program and the emergency response program.

EPA is developing a reporting mechanism and form to collect RMPs in a way that encourages electronic submission. This will make risk management planning information available far more widely to the public and at a far lower cost than would traditional reporting. To support electronic submission and reduce the reporting burden, EPA has standardized the RMP requirements. With the exception of the executive summary, data elements will be primarily check-off boxes, yes/no answers, or numerical entries.

An "implementing agency" will oversee these requirements and receive the RMPs. It will audit and inspect a percentage of sources each year and require whatever revisions to the RMPs are necessary. Under CAA section 112(l), states may request that EPA delegate the authority to serve as the implementing agency to a state or local agency with the appropriate expertise, resources, and authority. States may implement their own programs, although the law demands that program requirements must be as stringent as EPA's and must include all EPA-regulated substances and processes. Approximately 30 per cent of the sources subject to the risk management program

requirements must also comply with Title V of the Clean Air Act, which requires permits for emissions of air pollutants. Section 112(r) is an applicable requirement for Title V permits.

Help for Small Business

Small and medium-sized enterprises may receive information about CAA section 112(r) through the Small Business Assistance Program in each state, through the Federal Small Business Assistance Program, through the network of Small Business Development Centers across the country, through the EPCRA Hotline, and through a range of electronic outlets.

To make compliance easier for small businesses, EPA is working with industry groups to develop model risk management programs. Initially, these model programs will be developed for ammonia refrigeration, propane handling, and water treatment operations. The RMP Offsite Consequence Analysis Guidance will eliminate the need for covered small operations to invest in computer modeling programs and to answer complex technical questions (e.g., how to model liquefied gases) related to this element of the hazard assessment.

Looking Ahead...

As this final rule is implemented, EPA plans to publish general technical guidance, guidance for states on implementation, guidance for Local Emergency Planning Committees on ways to use RMP information in the community, and additional model plans for certain industry sectors and regulated substances. In addition, the Agency will produce training packages and disseminate training through a variety of educational outlets. Workshops, in co-operation with industry and engineering societies, will also be presented around the country, as well as teleconferences to introduce the new risk management planning requirements to a diversity of stakeholders.

◆◆◆

With risk management planning as the basis for accident prevention, everybody wins. Industry has an opportunity to demonstrate excellence in safety. Government can show effective, efficient leadership in developing sensible requirements. And communities will have a powerful right-to-know tool, as citizens work together toward reducing chemical risks to public health and the environment.

For More Information...

Contact the Emergency Planning and Community Right-to-Know Hotline

(800) 424-9346 or (703) 412-9810
TDD (800) 553-7672

Monday-Friday, 9 AM to 6 PM, eastern time

◆◆◆

Visit the CEPPO Home Page on the World Wide Web at:

http://www.epa.gov/swercepp/

Appendix IX
Prioritized List of Issues

Prioritized List of Issues Needing Attention to Mitigate/Eliminate the Potential of Catastrophic Process Plant Accidents from Y2K-Related Failures

Priority Order	Number Of Votes	Issues Needing Attention
1	24	Small and Medium-Sized Enterprises
2	16	Risk Management
3	15	Utility Issues
4	12	Responsive Communication Amongst Stakeholders
5	5	Equipment Testing
6	4	Y2K Fear and Over-Reaction
7	3	Incentives/Disincentives Associated with Regulations
8	2	Information Exchange Between Companies
		Training
		Emergency Response
		Backup power and fail-safe mode
9	1	Certification
		Contingency Plan Testing
		Inherent Safety
10	None	Employee Involvement
		Transportation
		Inventory Levels and Changes
		Global Concerns
		Market Forces

Note: This table was developed by participants at the Y2K Technical Workshop sponsored by the U.S. Chemical Safety and Hazard Investigation Board on December 18, 1998 in Washington, DC. Consequently, the results in this table reflect the biases, background, training, and education of the participants.